(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年7 月21 日 (21.07.2005)

PCT

(10) 国際公開番号
WO 2005/066803 A1

(51) 国際特許分類[7]: G06F 12/14, G06K 17/00, 19/073, H04L 9/10

(21) 国際出願番号: PCT/JP2004/019202

(22) 国際出願日: 2004 年12 月22 日 (22.12.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-001360 2004 年1 月6 日 (06.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 栗田 太郎 (KURITA, Taro) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

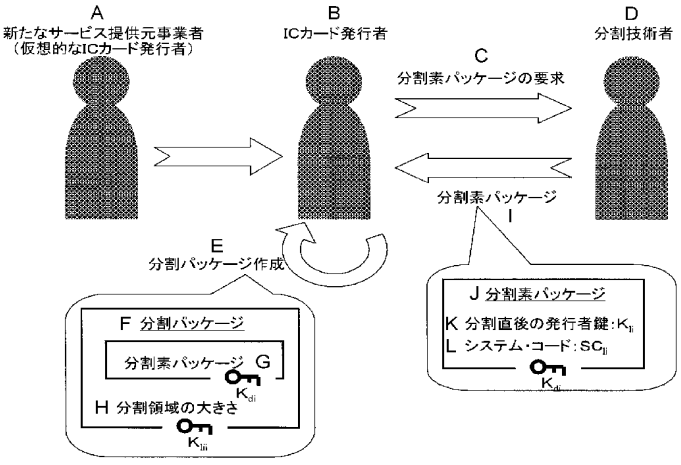
(74) 代理人: 山田 英治，外 (YAMADA, Eiji et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: DATA COMMUNICATING APPARATUS AND METHOD FOR MANAGING MEMORY OF DATA COMMUNICATING APPARATUS

(54) 発明の名称: データ通信装置及びデータ通信装置のメモリ管理方法



A... NEW SERVICE PROVIDER (VIRTUAL IC CARD ISSUER)
B... IC CARD ISSUER
C... REQUEST DIVISION ORIGINAL PACKAGE
D... DIVISION ENGINEER
E... MAKE DIVIDED PACKAGE
F... DIVIDED PACKAGE
G... DIVISION ORIGINAL PACKAGE
H... SIZE OF DIVIDED AREA
I... DIVISION ORIGINAL PACKAGE
J... DIVISION ORIGINAL PACKAGE
K... ISSUER KEY IMMEDIATELY AFTER DIVISION: K_{li}
L... SYSTEM CODE: SC_{li}

(57) Abstract: File systems for respective service providers are assigned to a single memory area, and a single information storage medium is shared among the plurality of providers. In the initial state, an IC card issuer manages the whole memory area. If another provider is to divide the memory area to make a new file system, it requested to acquire both a right of dividing the memory area and an authentication of the IC card issuer. After the file division, an access to the file system needs to acquire an authentication of the provider that made the file division. When utilizing any service, the user can easily use the IC card as if the IC card were issued by the corresponding provider itself.

(57) 要約: 単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一の情報記憶媒体を複数の事業者で共有する。 初期状態ではＩＣカード発行者がメモリ領域全体を管理している。他のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割するとき、メモリ領域の分割権限とＩＣカード発行者に対する認証の双方が要求される。ファイル分割後は、ファイル・システムへのアクセスは、分割したサービス提供元事業者への認証が要求される。ユーザにとっては、各サービス利用時において事業者自らが発行したＩＣカードであるかのような使い勝手が確保される。

WO 2005/066803 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

データ通信装置及びデータ通信装置のメモリ管理方法

技術分野

[0001] 本発明は、比較的大容量のメモリ領域を備えたデータ通信装置及びデータ通信装置のメモリ管理方法に係り、特に、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを行なうデータ通信装置及びデータ通信装置のメモリ管理方法に関する。

[0002] さらに詳しくは、本発明は、メモリ領域上にサービス提供元事業者用のファイル・システムを割り当てて、ファイル・システム内で当該事業者によるサービス運用のための情報を管理するデータ通信装置及びデータ通信装置のメモリ管理方法に係り、特に、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供するデータ通信装置及びデータ通信装置のメモリ管理方法に関する。

背景技術

[0003] 局所でのみ適用可能な無線通信手段の一例として、非接触ICカードを挙げることができる。

[0004] この種の無線通信には、一般に、電磁誘導の原理に基づいて実現される。すなわち、メモリ機能を有するICカードと、ICカードのメモリに対して読み書きアクセスをするカード・リーダ／ライタで構成され、1次コイルとしてのICカード側のループ・コイルと2次コイルとしてのカード・リーダ／ライタ側のアンテナが系として1個のトランスを形成している。そして、カード・リーダ／ライタ側からICカードに対して、電力と情報を同じく電磁誘導作用により伝送し、ICカード側では供給された電力によって駆動してカード・リーダ／ライタ側からの質問信号に対して応答することができる。

[0005] カード・リーダ／ライタ側では、アンテナに流す電流を変調することで、ICカード上のループ・コイルの誘起電圧が変調を受けるという作用により、カード・リーダ／ライタからICカードへのデータ送信を行なうことができる。また、ICカードは、ループ・コイル

の端子間の負荷変動により、ICカード・リーダ／ライタ側のアンテナ端子間のインピーダンスが変化してアンテナの通過電流や電圧が変動するという作用により、カード・リーダ／ライタへの返信を行なう。

[0006] ICカードに代表される非接触・近接通信システムは、操作上の手軽さから、広範に普及している。例えば、暗証コードやその他の個人認証情報、電子チケットなどの価値情報などをICカードに格納しておく一方、キャッシュ・ディスペンサやコンサート会場の出入口、駅の改札口などにカード・リーダ／ライタを設置しておく。そして、利用者がICカードをカード・リーダ／ライタにかざすことで、非接触でアクセスし、認証処理を行なうことができる。

[0007] 最近では、微細化技術の向上とも相俟って、比較的大容量のメモリ空間を持つICカードが出現している。大容量メモリ付きのICカードによれば、複数のアプリケーションを同時に格納しておくことができるので、1枚のICカードを複数の用途に利用することができる。例えば、1枚のICカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、多数のアプリケーションを格納しておくことにより、1枚のICカードをさまざまな用途に適用させることができる。ここで言う電子マネーや電子チケットは、利用者が提供する資金に応じて発行される電子データを通じて決済（電子決済）される仕組み、又はこのような電子データ自体を指す。

[0008] ICカードの一般的な使用方法は、利用者がICカードをカード・リーダ／ライタをかざすことによって行なわれる。カード・リーダ／ライタ側では常にICカードをポーリングしており外部のICカードを発見することにより、両者間の通信動作が開始する。

[0009] このとき、利用者が暗証番号をICカード・リーダ側に入力して、入力された暗証番号をICカード上に格納された暗証番号と照合することで、ICカードとICカード・リーダ／ライタ間で本人確認又は認証処理が行なわれる。ICカード・アクセス時に使用する暗証番号のことを、特にPIN（Personal Identification Number）と呼ぶ。そして、本人確認又は認証処理に成功した場合には、例えば、ICカード内に保存されているアプリケーションの利用、すなわち、アプリケーションに割り当てられているサービス・メモリ領域へのアクセスが可能となる（本明細書中では、アプリケーションに割り当てら

れているメモリ領域を「サービス・メモリ領域」と呼ぶ)。サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

[0010] さらに、ICカードやカード用リーダ／ライタ(カード読み書き装置)が無線・非接触インターフェースの他に、外部機器と接続するための有線インターフェース(図示しない)を備えることにより、ICカードやリーダ／ライタの機能を携帯電話機、PDA(Personal Digital Assistance)やCE(Consumer Electronics)機器、パーソナル・コンピュータなどの各デバイスにICカード及びカード・リーダ／ライタのいずれか一方又は双方の機能を装備することができる。このような場合、ICカード技術を汎用性のある双方向の近接通信インターフェースとして利用することができる。

[0011] 例えば、コンピュータや情報家電機器のような機器同士で近接通信システムが構成される場合には、ICカードを利用した通信が一対一で行なわれる。また、ある機器が非接触ICカードのような機器以外の相手デバイスと通信することも可能であり、この場合においては、1つの機器と複数のカードにおける一対多の通信を行なうアプリケーションも考えられる。

[0012] また、電子決済を始めとする外部との電子的な価値情報のやり取りなど、ICカードを利用したさまざまなアプリケーションを、情報処理端末上で実行することができる。例えば、情報処理端末上のキーボードやディスプレイなどのユーザ・インターフェースを用いてICカードに対するユーザ・インタラクションを情報処理端末上で行なうことができる。また、ICカードが携帯電話機と接続されていることにより、ICカード内に記憶された内容を電話網経由でやり取りすることもできる。さらに、携帯電話機からインターネット接続して利用代金をICカードで支払うことができる。

[0013] あるサービス提供元事業者用のファイル・システムをICカードの内蔵メモリに割り当てて、このファイル・システム内で当該事業者によるサービス運用のための情報(例えば、ユーザの識別・認証情報や残りの価値情報、使用履歴(ログ)など)を管理することにより、従来のプリペイド・カードや店舗毎のサービス・カードに置き換わる、非接触・近接通信を基調とした有用なサービスを実現することができる。

[0014] 従来、サービス提供元事業者毎にICカードが個別に発行され、ユーザの利用に供

されていた。このため、ユーザは、享受するサービス毎にICカードを取り揃え、携帯しなければならなかった。これに対し、比較的大容量のメモリ空間を持つICカードによれば、単一のICカードの内蔵メモリに複数のサービスに関する情報を記録するだけの十分な容量を確保することができる。

[0015] ここで、プリペイド・カードなどの前払式証票に関しては、その発行などの業務の適正な運営を確保して、前払式証票の購入者らの利益保護と前払式証票の信用維持を図ることを主な目的として、前払式証票の発行者に対して登録やその他の必要な規制を行なうための「前払式証票の規制等に関する法律」(通称、「プリカ法」)が制定されており、利用者の便宜や流通秩序維持などの目的で、ロゴや問い合わせ先などの所定事項をプリペイド・カード上(券面)に表示することが義務付けられている(同法第12条を参照のこと)。

[0016] ICカードのメモリ機能に前払情報を格納することによってプリペイド・カードを実現する場合、法で規制される必要な情報を媒体上に印刷しておくことにより、単一のサービスしか提供できなくなる。これに対し、ICカード機能を携帯電話機のような表示機能を持つ携帯端末上で利用する場合には、希望する価値情報に関連する情報を画面表示させることにより(例えば、特許文献1を参照のこと)、上記の法規制を満たすことができ、複数のサービス提供元事業者による共有が可能となる。したがって、サービス提供元事業者においてはカード発行の負担が軽減するとともに、ユーザにとっては携帯して管理するICカードの枚数を削減することができる。

[0017] ところが、複数のサービス提供元事業者間で単一のメモリ領域を共有した場合、あるサービス提供元事業者が使用するメモリ領域を、メモリを共用する別の事業者から自由にアクセスできるようにすると、事業者毎に設定される価値情報が他の事業者によって不正利用を許してしまうことになりかねない。この結果、事業者側では健全なサービス提供を行なえなくなり、また、ユーザにとっては換金性の高い価値情報が流出の危機にさらされ、経済的な損害を被る。

[0018] したがって、ICカードを複数のサービス提供元事業者間で共用する場合には、ユーザにとっては各サービス利用時において事業者自らが発行したICカードであるかのような使い勝手を確保する一方、メモリ領域上の事業者毎の情報をセキュアに管理

する機構を備えている必要がある。

[0019] 特許文献1:特開2003−141434号公報

発明の開示

発明が解決しようとする課題

[0020] 本発明の目的は、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを好適に行なうことができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することにある。

[0021] 本発明のさらなる目的は、ユーザにとっては各サービス利用時において事業者自らが発行したICカードであるかのような使い勝手を確保する一方、メモリ領域上の事業者毎の情報をセキュアに管理する機構を備え、単一のICカードを複数のサービス提供元事業者間で共用することができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することにある。

課題を解決するための手段

[0022] 本発明は、上記課題を参酌してなされたものであり、メモリ空間を備え、1以上のファイル・システムに分割して管理するデータ通信装置であって、

分割権限鍵を保持し、前記メモリ空間のファイル・システムへのアクセスを管理する制御手段と、

第1のサービス提供元の発行者鍵を保持し、メモリ空間上に割り当てられた第1のファイル・システムとを備え、

第2のサービス提供元の発行者鍵を前記分割権限鍵で暗号化した分割素パッケージと新規のファイル・システムに関する情報を含んだデータ・ブロックを第1のサービス提供元の発行者鍵で暗号化した分割パッケージを受信すると、

前記第1のファイル・システムにおいて分割パッケージを解読して分割素パッケージを取り出し、

前記制御手段において分割素パッケージを解読し、前記メモリ空間の空き領域から、新規のファイル・システムに関する情報に従って、第2のサービス提供元の発行者鍵を保持した第2のファイル・システムを分割する、

ことを特徴とするデータ通信装置である。ここで言うデータ通信装置は、無線通信部

、及びデータ送受信機能とデータ処理部を有するICチップを内蔵する非接触ICカード、表面に端子を有する接触ICカード、接触／非接触ICカードと同様の機能を有するICチップを携帯電話機、PHS（Personal Handyphone System）、PDA（Personal Digital Assistance）などの情報通信端末装置に内蔵した装置である。このデータ通信装置は、EEPROMなどのデータ蓄積メモリを含むメモリ領域とデータ処理部を有するとともに、データ通信機能を有するものである。携帯電話機などの場合は、ICチップを内蔵するICカードなどの外部記憶媒体を着脱可能に構成してもよい。また、携帯電話会社が発行する契約者情報を記録したSIM（Subscriber Identity Module）機能をICチップに搭載してもよい。データ通信装置は、インターネット等の情報通信ネットワークを介してデータ通信を行なっても、外部端末装置と有線あるいは無線で直接データ通信を行なってもよい。

[0023] 本発明は、ICカードが持つ耐タンパ性と認証機能を利用して、価値情報のやり取りなどを含んだセキュリティが要求されるサービスを提供するものである。より具体的には、ICカード内の単一のメモリ領域を複数のサービス提供元事業者間で共有し、サービス提供元事業者においてはカード発行の負担が軽減するとともに、ユーザにとっては携帯して管理するICカードの枚数を削減するものである。

[0024] ここで、複数のサービス提供元事業者間で単一のメモリ領域を共有した場合、あるサービス提供元事業者が使用するメモリ領域を、メモリを共用する別の事業者から自由にアクセスできるようにすると、事業者毎に設定される価値情報が他の事業者によって不正利用を許してしまう、という問題がある。

[0025] 本発明では、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供するようにした。メモリ領域をファイル・システムに分割することにより、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システム（すなわち他のサービス提供元事業者）からのアクセス（不正侵入）を好適に排除することができる。

[0026] ICカード内のメモリ領域は、初期状態では、元のICカード発行者がメモリ領域全体を管理している。ICカード発行者以外のサービス提供元事業者がメモリ領域から新

たなファイル・システムを分割するに際しては、メモリ領域の分割権限と、元のICカード発行者に対する認証の双方が要求される。

[0027] 例えば、新たなサービス提供元事業者としての第2のサービス提供元がICカードのメモリ領域上でファイル・システムを分割したい場合には、その事前処理として、第1のサービス提供元としての元のカード発行者に対して、メモリ領域の使用に関する許可を求める。そして、元のカード発行者はメモリ領域の使用、すなわちメモリの空き領域からファイル・システムの分割をすることを許可する場合には、分割技術管理者から、ファイル・システムの分割に必要となる「分割素パッケージ」を取得する。

[0028] ここで、分割技術管理者は、新たに分割して作成されるファイル・システムの領域鍵K_{li}、システム・コードSC_iを割り振り、これらで構成されるデータ・ブロックを分割権限鍵K_dで暗号化して分割素パッケージを作成し、これをカード発行者に渡す。カード発行者自身は、分割権限鍵K_dを保持していないので渡された分割素パッケージを解読したりこれを改竄したりすることはできない。

[0029] そして、カード発行者は、取得した分割素パッケージと、新たなサービス提供元事業者に使用を許可する分割領域の大きさ(ブロック数)とからなるデータ・ブロックをさらに自己の発行者鍵K_lで暗号化して、分割パッケージを作成する。分割パッケージは、カード発行者鍵K_lで暗号化されているので、第3者が分割パッケージを解読したり分割領域の大きさなどを改竄したりすることはできない。

[0030] カード発行者は、分割パッケージを用いてファイル・システムの分割要求を行なう。分割要求がICカードのオペレーティング・システムに届くと、引数に含まれるエリアIDに基づいて、分割パッケージがカード発行者のファイル・システムへ渡され、カード発行者鍵K_lで解読され、分割素パッケージと分割領域の大きさが取り出される。

[0031] ICカードのオペレーティング・システムは、カード発行者のファイル・システムから分割素パッケージと分割領域の大きさを受け取ると、分割素パッケージを分割権限鍵K_dで解読して、分割直後の領域鍵(第2のサービス提供元のデフォルト発行者鍵)K_{li}と、システム・コードSC_iを取り出す。そして、要求されている分割領域の大きさ分の領域を分割し、この領域に発行者鍵K_{li}とシステム・コードSC_iを設定して、新たなファイル・システムとする。

[0032] そして、一旦分割されると、ファイル・システムへのアクセスは、元のICカードの発行者ではなく、ファイル・システム自体のサービス提供元事業者への認証が要求される。したがって、ユーザにとっては、各サービス利用時において事業者自らが発行したICカードであるかのような使い勝手を確保することができる。

[0033] このような分割操作を繰り返すことにより、ICカード内のメモリ領域は複数のファイル・システムが共存する構造となる。ファイル・システムの分割は、仮想的なICカードの発行である。

[0034] メモリ空間上の各ファイル・システムにはエリア識別情報が割り振られている。そして、外部からのアクセスは、アクセス先となるファイル・システムの発行者鍵で暗号化されたパッケージで構成されている。このような場合、前記制御手段は、エリア識別情報とパッケージを引数とする外部からのアクセス要求に対し、エリア識別情報を基に該当するファイル・システムへパッケージを渡すようになっている。そして、ファイル・システムは自身の発行者鍵でパッケージを解読する。

[0035] したがって、ファイル・システムを所有するサービス提供元事業者は、自己の発行者鍵を用いることで、ICカードの制御システムや元のカード発行者からも秘密を保持した状態でファイル・システムと通信することができる。すなわち、元のICカード発行者とは独立してセキュリティに関する脅威を分析、管理、並びに運用することができるようになる。

[0036] また、前記制御手段は、新規のファイル・システムを分割する際に、発行者鍵、エリア識別情報とともに、システム・コードを該ファイル・システムに設定する。

[0037] このような場合、各サービス提供元は自己のシステム・コードを引数にしたエリア識別情報の取得要求を行なう。また、前記制御手段は、該要求に応答して、各ファイル・システムをポーリングし、該当するファイル・システムからエリア識別情報を取得し、これを要求元へ返すようにする。サービス提供元は、自己のシステム・コードを管理するだけでよく、ファイル・システムへアクセスする際に逐次的にエリア識別情報を取得し、これを引数としてアクセス要求することができる。

[0038] また、サービス提供元は、前記メモリ空間上に自己のファイル・システムを取得した後、分割時にデフォルトの発行者鍵やシステム・コードが設定される場合、これらを書

き換えるようにしてもよい。この結果、サービス提供元は、ファイル・システムの分割を管理する分割技術管理者とは独立して、自己のファイル・システムのセキュリティに関する脅威を分析、管理、並びに運用することができるようになる。

発明の効果

[0039] 本発明によれば、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを好適に行なうことができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することができる。

[0040] また、本発明によれば、ユーザにとっては各サービス利用時において事業者自らが発行したICカードであるかのような使い勝手を確保する一方、メモリ領域上の事業者毎の情報をセキュアに管理する機構を備え、単一のICカードを複数のサービス提供元事業者間で共用することができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することができる。

[0041] また、本発明によれば、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供することができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することができる。

[0042] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

発明を実施するための最良の形態

[0043] 以下、図面を参照しながら本発明の実施形態について詳解する。

[0044] 本発明は、ICカードが持つ耐タンパ性と認証機能を利用して、価値情報のやり取りなどを含んだセキュリティが要求されるサービスを提供するものであり、より具体的には、ICカード内の単一のメモリ領域を複数のサービス提供元事業者間で共有し、サービス提供元事業者においてはカード発行の負担が軽減するとともに、ユーザにとっては携帯して管理するICカードの枚数を削減するものである。

[0045] ここで、複数のサービス提供元事業者間で単一のメモリ領域を共有した場合、あるサービス提供元事業者が使用するメモリ領域を、メモリを共用する別の事業者から自由にアクセスできるようにすると、事業者毎に設定される価値情報が他の事業者によ

って不正利用を許してしまう、という問題がある。

[0046] 本発明では、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供するようにした。メモリ領域をファイル・システムに分割することにより、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システム(すなわち他のサービス提供元事業者)からのアクセス(不正侵入)を好適に排除することができる。

[0047] ICカード内のメモリ領域は、初期状態では、元のICカード発行者がメモリ領域全体を管理している。ICカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割するに際しては、メモリ領域の分割権限と、元のICカード発行者に対する認証の双方が要求される。

[0048] そして、一旦分割されると、ファイル・システムへのアクセスは、元のICカードの発行者ではなく、ファイル・システム自体のサービス提供元事業者への認証が要求される。したがって、ユーザにとっては、各サービス利用時において事業者自らが発行したICカードであるかのような使い勝手を確保することができる。

[0049] ここで、まず、ICカード及びカード読み書き装置間の非接触データ通信の仕組みについて、図1及び図2を参照しながら説明する。

[0050] カード読み書き装置とICカード間の無線通信は、例えば電磁誘導の原理に基づいて実現される。図1には、電磁誘導に基づくカード読み書き装置とICカードとの無線通信の仕組みを概念的に図解している。カード読み書き装置は、ループ・コイルで構成されたアンテナL_{RW}を備え、このアンテナL_{RW}に電流I_{RW}を流すことでその周辺に磁界を発生させる。一方、ICカード側では、電気的にはICカードの周辺にループ・コイルL_cが形設されている。ICカード側のループ・コイルL_c端にはカード読み書き装置側のループ・アンテナL_cが発する磁界による誘導電圧が生じて、ループ・コイルL_c端に接続されたICカードの端子に入力される。

[0051] カード読み書き装置側のアンテナL_{RW}とICカード側のループ・コイルL_cは、その結合度は互いの位置関係によって変わるが、系としては1個のトランスを形成していると捉えることができ、ICカードの読み書き動作を図2に示すようにモデル化することができ

る。

[0052] カード読み書き装置側では、アンテナL_{RW}に流す電流I_{RW}を変調することによって、ICチップ上のループ・コイルL_cに誘起される電圧V_Oは変調を受け、そのことを利用してカード読み書き装置はICカードへのデータ送信を行うことができる。

[0053] また、ICカードは、カード読み書き装置へ返送するためのデータに応じてループ・コイルL_cの端子間の負荷を変動させる機能(Load Switching)を持つ。ループ・コイルL_cの端子間の負荷が変動すると、カード読み書き装置側ではアンテナ端子間のインピーダンスが変化して、アンテナL_{RW}の通過電流I_{RW}や電圧V_{RW}の変動となって現れる。この変動分を復調することで、カード読み書き装置はICカードの返送データを受信することができる。

[0054] すなわち、ICカードは、カード読み書き装置からの質問信号に対する応答信号に応じて自身のアンテナ間の負荷を変化させることによって、カード読み書き装置側の受信回路に現れる信号に振幅変調をかけて通信を行なうことができる訳である。

[0055] ICカードは、カード型のデータ通信装置であってもよいし、いわゆるICカード機能を有する集積回路チップを携帯電話機等の情報通信端末機器に内蔵してもよい(ICカードが機器に内蔵される場合であっても、機器に着脱可能に構成される場合であっても、本明細書中では便宜上「ICカード」と呼ぶ場合がある。)また、ICカード機能を有する集積回路チップは、例えば携帯電話機やPDAなどの携帯端末、あるいはパーソナルコンピュータ(PC)などの情報処理端末に搭載されて外部機器とデータ通信を行なう。この場合、リーダ/ライタ装置と有線あるいは無線で接続するためのインターフェース以外に、外部機器接続用のインターフェースを備えている。

[0056] 図3には、本発明の実施形態にかかるデータ通信装置のハードウェア構成を示している。このデータ通信装置は、通信用のアンテナを追加して内部の不揮発性メモリにアクセスすることができるICカード機能と、ICカード機能を有する外部装置に電力を供給するとともにデータ交換を実現するリーダ/ライタ機能を有し、カード機能アナログ回路部30、データ処理部40と、リーダ/ライタ機能アナログ回路部50を有するICチップを内蔵している。同図に示した例では、ICカードはカード読み書き機能も併せて備えているが、カード読み書き機能は本発明の必須の構成要素ではない。

[0057] カード機能アナログ回路部30では、アンテナ32で受信された搬送波は、整流器31で整流された後、データ処理部40内の信号処理部44に供給されるとともに、シリアル・レギュレータ33を介して論理回路38に供給されている。

[0058] 論理回路38は、起動信号入力端子P_{on}からの起動信号の入力に応答して起動し、シリアル・レギュレータ33からの電圧、並びに電源端子V_{DD}からの入力電圧を制御して、ICカードで使用するための適正な電源電圧を供給するようになっている。

[0059] シリアル・レギュレータ33は、入力電圧の如何に拘わらず、出力電圧をほぼ一定に保つようになっている。すなわち、入力電圧が高いときには、内部インピーダンスを高くして、逆に入力電圧が低いときには内部インピーダンスを低くすることによって、電圧を保つ動作を可能とする。

[0060] 電圧検出器39は、論理回路38に接続された電源電圧監視回路接続用端子V_{BT}からの入力端子電圧を監視して、外部電源の電圧が所定電圧を下回った場合には外部電源の使用を禁止する信号を論理回路38に出力するようになっている。

[0061] また、カード機能アナログ回路部30において、アンテナ32から入力された電波は、搬送波検出器34で受信電波中に搬送波が含まれているか否かが判断され、含まれている場合には、搬送波検出信号VRが論理回路38に出力される。論理回路38は、さらに、データ処理部40に対して搬送波が検出された旨の信号を出力することができる。

[0062] クロック抽出器35は、アンテナ32から入力された電波からクロックを抽出して、これをクロック選択器36に供給する。また、クロック発振器37は、例えばICカード外に配設された水晶振動子で構成され、ICカード上で使用される駆動周波数のクロックを発生して、クロック選択器36に供給する。クロック選択器36は、クロック抽出器35から供給されたクロック、又は、クロック発振器37から供給されたクロックのいずれか一方を選択して、ICカード内の各部に供給する。

[0063] リーダ／ライタ機能アナログ回路部50は、送信アンプ51と、受信信号検出器53と、受信アンプ・フィルタ54と、送受信用のアンテナ52及び55で構成される。

[0064] データを送信するときは、データ処理部40の信号処理部44によって変調並びにD／A変換されて、アナログ・ベースバンドにアップコンバートされた送信信号が送信ア

ンプを介してアンテナ51から送出される。また、アンテナ52から受信された信号は、受信信号検出器53によって検出され、受信アンプ54で増幅されてから、信号処理部44に供給される。信号処理部44は、アナログ・ベースバンド信号にダウンコンバートし、D／A変換並びに復調処理して、ディジタル・データを再現する。

[0065] なお、ICカードとカード読み書き装置の間のカード読み書き動作は、図1及び図2を参照しながら既に説明した通りである。

[0066] データ処理部40は、先述の信号処理部44の他、CPU（Central Processing Unit）45と、DES（Data Encryption Standard）などを利用したデータ暗号化エンジン46と、CRC（Cyclic Redundancy Check）などを利用したエラー訂正部47と、RAM（Random Access Memory）41と、ROM（Read Only Memory）42と、EEPROM（Electrically Erasable and Programmable ROM）43と、UARTインターフェース48と、I^2Cインターフェース49とを備えており、各部は内部バスによって相互接続されている。

[0067] CPU45は、ICカード内の動作を統括的に制御するメイン・コントローラであり、ICカード用オペレーティング・システム（OS）によって提供される実行環境（後述）下で、例えばROM42（あるいはEEPROM43）に格納されたプログラム・コードを実行するようになっている。例えば、CPU45は、カード機能アナログ回路部30やリーダ／ライタ機能アナログ回路部50を介して送受信されるデータに関するアプリケーションを実行するようになっている。

[0068] 信号処理部44は、カード機能アナログ回路部30やリーダ／ライタ機能アナログ回路部50を介して送信されるデータの変調、D／A変換、アップコンバートなどの処理や、受信したデータのダウンコンバート、A／D変換、復調などの処理を行なう。

[0069] DESエンジン46は、カード機能アナログ回路部30やリーダ／ライタ機能アナログ回路部50を介して送受信されるデータを手順公開型の秘密鍵暗号により暗号化及び復号化処理する。

[0070] CRC47は、カード機能アナログ回路部30やリーダ／ライタ機能アナログ回路部50を介して受信したデータの巡回冗長検査を行なう。

[0071] UART48並びにI^2Cインターフェースは、ICカードを携帯電話器やPDA、パーソ

ナル・コンピュータなどの外部機器（図3には図示しない）に接続するための外部有線インターフェースを構成する。このうちUART（Universal asynchronous receiver transmitter）48は、コンピュータ内のパラレル信号をシリアル信号に変換したり、シリアル信号をパラレル信号に変換したりする機能を持つ。

[0072] RAM41は書き込み可能なメモリ装置であり、CPU41はRAM41を作業領域としてプログラムを実行する。RAM41が提供するメモリ空間はアドレス可能であり、CPU41や内部バス上の各装置はこのメモリ空間にアクセスすることができる。

[0073] EEPROM43は、消去動作とともに新規のデータの書き込みを行なう不揮発性のメモリ装置である。本明細書で言うICカード内蔵のメモリ領域は、基本的にはEEPROM43内の書き込み可能領域を指すものとする。

[0074] このメモリ領域は、1以上のファイル・システムで構成される。初期状態では、元のICカード発行者が管理する単一のファイル・システムによってメモリ領域が管理され、その後、ICカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割する。EEPROM43上のメモリ領域のファイル分割や、分割後のアクセス動作の詳細については、後に詳解する。

[0075] 図4には、本実施形態に係るICカードにおけるメモリ領域の制御システム構成を模式的に示している。同図に示すように、この制御システムは、基本的には、オペレーティング・システム内のサブシステムとして実装され、プロトコル・インターフェース部と、OS中枢部と、ファイル・システムで構成される。

[0076] プロトコル・インターフェース部は、UART48などの外部機器インターフェースを介した外部機器からのファイル・システムへのアクセス要求、あるいは非接触ICカード・インターフェースを介したカード読み書き装置からファイル・システムへのアクセス要求のハンドリングを行なう。

[0077] OS中枢部では、ファイル・システムとやり取りするデータのデコード／エンコード、CRCなどによるエラー訂正、EEPROM43のブロック毎の書き換え回数管理、PIN照合、相互認証などを行なう。

[0078] さらに、OS中枢部は、ファイル・アクセス時におけるPIN照合や相互認証、ファイルのリード／ライトなどのファイル・システムへの幾つかのAPI（Application Program

ming Interface)を備えている。

[0079] ファイル・システム・エンティティとしてのEEPROM43へ物理アクセスを行なう。EEPROMなどのメモリ・デバイスへの物理アクセス動作自体は当業界において周知なので、ここでは説明を省略する。

[0080] EEPROM43上に展開されるメモリ領域は、1以上のファイル・システムで構成される。初期状態では、元のICカード発行者が管理する単一のファイル・システムによってメモリ領域が管理されている。ICカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割する際には、メモリ領域の分割権限と、元のICカード発行者に対する認証の双方が要求される。そして、一旦分割されると、ファイル・システムへのアクセスは、元のICカードの発行者ではなく、ファイル・システム自体のサービス提供元事業者への認証が要求される。ファイル・システムの分割は、仮想的なICカードの発行である。

[0081] OSは、分割を許可するための分割権限鍵K_dを管理している。また、ファイル・システム毎に、発行者(元のICカード発行者、又はファイル分割した事業者)の発行者鍵K_Iと、システム・コードと、ファイル領域を識別するエリアIDが管理されている。

[0082] ファイル・システムへのアクセスは、ポーリングによるエリアIDの要求と、相互認証という手続きを経て行なわれる。ファイル・システムの発行者(元のファイル・システムの場合はカード発行者、分割後のファイル・システムを使用するサービス提供元事業者)は、まず、自身が判っているシステム・コードを引数にしてファイル・システムに対するポーリングを行なうことによって、該当するファイル・システムのメモリ領域上でのエリアIDを取得することができる。次いで、このエリアIDと発行者鍵K_Iを用いて相互認証を行なう。そして、相互認証が成功裏に終わると、ファイル・システムへのアクセスが許可される。ファイル・システムへのアクセスは、発行者と該当するファイル・システムに固有の発行者鍵K_Iを用いた暗号化通信により行なわれるので、他のファイル・システムが無関係のデータを取り込んだり、発行者以外がファイル・システムへ無断で読み書きしたりすることはできない。

[0083] 図5には、比較的大容量のICカードを用いて実現される、電子マネーや電子チケット、その他の価値情報を運用するサービス提供システムの全体的構成を模式的に示

している。

[0084] 図示のシステム1は、例えば、ICカード発行者21が使用する発行者用通信装置11と、カード記憶領域運用者22が使用する運用者用通信装置12と、装置製造者23が使用する製造者用通信装置13と、カード記憶領域使用者24が使用する記憶領域分割装置14及び運用ファイル登録装置15とで構成される。

[0085] システム1では、ICカード発行者21がカード所有者26にICカード16を発行した場合に、所定の条件に基づいて、カード記憶領域使用者24によって提供されるサービスに係わるファイル・データをICカード16に登録し、カード所有者26が単体のICカード16を用いて、ICカード発行者21及びカード記憶領域使用者24の双方のサービスを受けることを可能にするものである。

[0086] 図5に示すように、システム1では、発行者用通信装置11、運用者用通信装置12、製造者用通信装置13、記憶領域分割装置14及び運用ファイル登録装置15が、ネットワーク17を介して接続される。

[0087] ICカード発行者21は、ICカード16の発行を行なう者であり、ICカード16を用いて自らのサービスを提供する。

[0088] カード記憶領域運用者22は、ICカード発行者21からの依頼を受けて、ICカード発行者21が発行したICカード16内の記憶部(半導体メモリ)に構成される記憶領域のうち、ICカード発行者21が使用しない記憶領域をカード記憶領域使用者24に貸し出すサービスを行なう者である。

[0089] 装置製造者23は、カード記憶領域運用者22から依頼を受けて、記憶領域分割装置14を製造し、カード記憶領域使用者24に納品する者である。

[0090] カード記憶領域使用者24は、カード記憶領域運用者22に依頼を行ない、ICカード16の記憶領域を使用して自らの独自のサービスを提供する者であり、メモリ領域を分割して新たなファイル・システムを作成するサービス提供元事業者(前述)に相当し、自己のファイル・システムを利用して自身のサービス提供を行なう。

[0091] カード所有者26は、ICカード発行者21からICカード16の発行を受け、ICカード発行者21が提供するサービスを受ける者である。カード所有者26は、ICカード16の発行後に、カード記憶領域使用者24が提供するサービスを受けることを希望する場合

には、記憶領域分割装置14及び運用ファイル登録装置15を用いて、カード記憶領域使用者24のサービスに係わるファイル・データをICカード16に記憶し、その後、カード記憶領域使用者24のサービスを受けることができるようになる。

[0092] システム1は、ICカード発行者21のサービスと、カード記憶領域使用者24のサービスとを単体のICカード16を用いて提供するに当たって、ICカード発行者21及びカード記憶領域使用者24のサービスに係わるファイル・データが記憶される記憶領域に、権限を有しない他人によって不正にデータの書き込み及び書き換えなどが行なわれることを困難にする構成を有している。

[0093] ICカード16は、その字義通り、カード型のデータ通信装置であってもよいし、いわゆるICカード機能が実装された半導体チップを内蔵した携帯電話機(あるいはその他の携帯端末やCE機器)として具現化されることもある。

[0094] なお、図5では、それぞれ単数のICカード発行者21、カード記憶領域使用者24及びカード所有者26がある場合を例示したが、これらは、それぞれ複数であってもよい。

[0095] 本実施形態では、ICカードの単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供する。このような分割ファイル・システム構成により、元のカード発行者が利用するメモリ領域の他に、元のカード発行者の許可を得て特定のサービス提供元事業者が利用可能となるメモリ領域と、元のカード発行者の許可を得て複数の事業者間で共通に利用可能となるメモリ領域を運用することができる。

[0096] 特に、元のカード発行者が利用するファイル・システム以外に、各サービス提供元事業者が個別に利用可能となる1以上のファイル・システムを運用する場合、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システム(すなわち他のサービス提供元事業者)からのアクセス(不正侵入)を好適に排除することができる。

[0097] ここで、図6ー図9を参照しながら、ICカード内のメモリ領域の運用形態について説明する。

[0098] 図6には、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示している。元のカード発行者のシステム・コードSC1は、システム・コードの管理機構が付与する。外部機器又はプログラムがカード発行者のファイル・システムにアクセスする場合は、SC1を識別コード(すなわち、要求コマンドの引数)とする。

[0099] 図7には、カード発行者が自らのファイル・システムの空き領域の内で、ある範囲のメモリを領域管理者に貸与(又は譲渡)することが許可できることを示している。この段階では, まだメモリ領域上のファイル・システムに対して分割が行なわれている訳ではない。カード発行者は、自らのファイル・システムに空き領域はあるうちは、複数の領域管理者に対して、メモリを貸与することを許可できる。例えば、4ビットのシステム・コードでファイル・システムを識別するという実装では、最大16分割(15回まで分割)することができる。

[0100] 図8には、他のサービス提供元事業者が、カード発行者から許可された領域においてメモリ領域を分割し、新たなファイル・システムを生成した状態を示している。この新規ファイル・システムには、システム・コードの管理機構からシステム・コードSC2が付与されている。外部機器又はプログラムが、当該メモリ領域管理者(サービス提供元事業者)の運用するファイル・システムにアクセスする場合は、SC2を識別コード(要求コマンドの引数)とする。

[0101] 図9には、共通領域管理者が、カード発行者から許可された領域において、共通領域のシステム・コードSC0でメモリを分割した状態を示している。外部機器又はプログラムがこの共通領域管理者の運用領域であるファイル・システムにアクセスする場合には、そのシステム・コードSC0を識別コード(要求コマンドの引数)とする。

[0102] 続いて、メモリ領域を分割して新たなファイル・システムを作成するための手続きについて詳解する。

[0103] 図10には、ファイル・システムを分割する際の事前処理について図解している。新たなサービス提供元事業者がICカードのメモリ領域上でファイル・システムを分割したい場合には、その事前処理として、当該事業者は、カード発行者に対してメモリ領域の使用に関する許可を求める。そして、カード発行者はメモリ領域の使用、すなわ

ちファイル・システムの分割を許可する場合には、分割技術管理者から、ファイル・システムの分割に必要となる「分割素パッケージ」を取得する。

[0104] 分割技術管理者は、ICカードを製造又は製造出荷した後にICカード内のメモリ領域の管理を担うカード記憶領域運用者22に相当し、新たなサービス提供元事業者は、カード記憶領域使用者14に相当する(図5を参照のこと)。

[0105] 分割技術管理者は、ICカード内のメモリ領域上の各ファイル・システムのシステム・コードを採番する権限を持つとともに、ICカードの実行環境を提供するオペレーティング・システム内に格納されている分割権限鍵K_dを管理している。そして、分割技術管理者は、新たに分割して作成されるファイル・システムの領域鍵(当該領域を使用する新たなサービス提供元事業者(すなわち仮想的なICカードの発行者)の発行者鍵)K_{li}、システム・コードSC_iを割り振り(但し、iはi番目に分割されたファイル・システムであることを識別する添え字である)、これらで構成されるデータ・ブロックを分割権限鍵K_dで暗号化して分割素パッケージを作成し、これをカード発行者に渡す。

[0106] カード発行者自身は、分割権限鍵K_dを保持していないので、渡された分割素パッケージを解読したりこれを改竄したりすることはできない。

[0107] カード発行者は、取得した分割素パッケージと、新たなサービス提供元事業者に使用を許可する分割領域の大きさ(ブロック数)とからなるデータ・ブロックをさらに自己の発行者鍵K_lで暗号化して、分割パッケージを作成する。

[0108] 分割パッケージは、カード発行者並びにカード発行者のファイル・システムにおいて管理されているカード発行者鍵K_lで暗号化されているので、第3者が分割パッケージを解読したり分割領域の大きさなどを改竄したりすることはできない。

[0109] このような事前手続きを経て、カード発行者は、分割パッケージを取得し、これを用いてICカード内のメモリ領域のファイル・システムの分割要求を行なう。ここで、ファイル・システムへのアクセスは、ファイル・システムのエリアIDを引数にして行なわれるが、カード発行者はシステム・コードしか分からないので、ICカードに対してポーリングを行なうことによって、自己のファイル・システムのエリアIDを取得することができる。

[0110] 図11には、カード発行者がICカードに対してポーリングを行なう手続きを図解している。但し、カード発行者(あるいはその他の外部機器)とICカード間の通信は、図1

及び図2を参照しながら説明した電磁誘導作用に基づく非接触近距離通信インターフェースを利用しても、あるいはUART48やI^2C49などの有線インターフェースを利用して行なうようにしてもよい（以下、同様）。

[0111] カード発行者は、ICカードの実行環境であるオペレーティング・システムに対しポーリングして、自己のシステム・コードSCを引数にしたファイル・システムのエリアID要求を行なう。

[0112] この要求メッセージをトリガにして、要求元であるカード発行者と、ICカードの実行環境であるオペレーティング・システムの間で、複数往復にまたがる通信動作で構成される相互認証手続きを経て、要求に対する戻り値としてエリアIDがカード発行者へ返される。なお、相互認証手続きの構成についてはICカードの仕様毎に相違し、本発明の要旨には直接関連しないので、ここでは詳細な説明を省略する。

[0113] なお、分割により新たにファイル・システムを取得した新規のサービス提供元事業者（すなわち仮想的なカード発行者）の場合も、同様のポーリング手続きを経て自己のエリアIDを取得することになる。

[0114] カード発行者は、ICカードのオペレーティング・システムに対してファイル・システムの分割要求を行なう。この分割要求は、カード発行者のエリアIDと、分割パッケージを引数として行なわれる。分割パッケージはカード発行者鍵K_Iで暗号化されているので、第3者からは改竄されない。図12には、カード発行者がICカードに対して分割要求を行なう手続きを示している。また、図13には、ICカード上のメモリ領域が分割され、新たなファイル・システムが生成される様子を示している。カード発行者とICカード間の通信は、電磁誘導作用に基づく非接触近距離通信インターフェースを利用しても、あるいはUART48やI^2C49などの有線インターフェースを利用して行なわれる。

[0115] 分割要求がICカードのオペレーティング・システムに届くと、引数に含まれるエリアIDに基づいて、分割パッケージがカード発行者のファイル・システムへ渡され、カード発行者鍵K_Iで解読され、分割素パッケージと分割領域の大きさ（ブロック数）が取り出される。

[0116] ICカードのオペレーティング・システムは、カード発行者のファイル・システムから分割素パッケージと分割領域の大きさを受け取ると、分割素パッケージを分割権限鍵K

$_{d}$で解読して、分割直後の領域鍵（当該領域を使用する新たなサービス提供元事業者（すなわち仮想的なICカードの発行者）の発行者鍵）K_{li}と、システム・コードSC_{i}を取り出す。そして、カード発行者が所有する領域のみ使用領域のうち、要求されている分割領域の大きさ分の領域を分割し、さらにこの領域に発行者鍵K_{li}とシステム・コードSC_{i}を設定して、新たなファイル・システムとする。

[0117] このようなファイル・システムの分割処理が終わると、そのステータスが要求元であるカード発行者に返される。

[0118] このようにして、新たなサービス提供元事業者は、他のカード発行者が発行したICカードのメモリ領域上に自分専用のファイル・システムを確保することができ、あたかも自らICカードを発行した、すなわち仮想的なICカード発行者としてサービス提供事業を展開することが可能となる。

[0119] 但し、分割直後のファイル・システムの初期状態では、設定されている発行者鍵K_{li}やシステム・コードSC_{i}は分割技術管理者が設定したままの状態である。言い換えれば、新規のサービス提供元事業者は、自己のファイル・システムのセキュリティは、分割技術管理者に委ねられている部分があり、セキュリティに関する脅威を独立して分析、管理、運用することはできない。

[0120] そこで、新規のサービス提供元事業者は、ICカードのメモリ領域上に自己のファイル・システムを取得した後は、発行者鍵K_{li}とシステム・コードSC_{i}の再設定手続きを行なう必要がある。また、この再設定手続きに併せて、分割領域の大きさを調整するようにしてもよい。

[0121] 図14には、新規のサービス提供元事業者がICカードのメモリ領域上に自己のファイル・システムを取得した後に行なう、発行者鍵K_{li}とシステム・コードSC_{i}の再設定手続きを示している。但し、サービス提供元事業者とICカード間の通信は、電磁誘導作用に基づく非接触近距離通信インターフェースを利用しても、あるいはUART48や$I^{2}C$49などの有線インターフェースを利用して行なう。

[0122] サービス提供元事業者は、ICカードの実行環境であるオペレーティング・システムに対しポーリングして、分割直後のシステム・コードSC_{i}を引数にしたファイル・システムのエリアID要求を行なう。

[0123] この要求メッセージをトリガにして、サービス提供元事業者と、ICカードの実行環境であるオペレーティング・システムの間で、複数往復にまたがる通信動作で構成される相互認証手続きを経て、要求に対する戻り値として、分割時に分割技術管理者によって付与されたデフォルトのエリアIDが、サービス提供元事業者へ返される。なお、相互認証手続きの構成についてはICカードの仕様毎に相違し、本発明の要旨には直接関連しないので、ここでは詳細な説明を省略する。

[0124] この認証手続きに続いて、サービス提供元事業者は、ICカードのオペレーティング・システムに対して、デフォルトの発行者鍵K_{li}の変更要求を行なう。この鍵変更要求は、デフォルトのエリアIDと、鍵変更パッケージを引数として行なわれる。鍵変更パッケージはデフォルト発行者鍵K_{li}で暗号化されているので、第3者からは改竄されない。

[0125] 鍵変更要求がICカードのオペレーティング・システムに届くと、引数に含まれるエリアIDに基づいて、鍵変更パッケージが当該サービス提供元事業者のファイル・システムへ渡され、そのカード発行者鍵K_{li}で解読され、鍵変更パッケージが取り出される。そして、ファイル・システムのカード発行者鍵がK_{li}からK_{li}'に変更されると、そのステータスが要求元であるサービス提供元事業者に返される。

[0126] 続いて、サービス提供元事業者は、ICカードのオペレーティング・システムに対して、デフォルトのシステム・コードSC_iの変更要求を行なう。このシステム・コード変更要求は、デフォルトのエリアIDと、システム・コード変更パッケージを引数として行なわれる。システム・コード変更パッケージは新規の発行者鍵K_{li}'で暗号化されているので、第3者からは改竄されない。

[0127] システム・コード変更要求がICカードのオペレーティング・システムに届くと、引数に含まれるエリアIDに基づいて、鍵変更パッケージが当該サービス提供元事業者のファイル・システムへ渡され、そのカード発行者鍵K_{li}'で解読され、システム・コード変更パッケージが取り出される。そして、ファイル・システムのデフォルトのシステム・コードSC_iがSC_i'に変更されると、そのステータスが要求元であるサービス提供元事業者に返される。

[0128] 続いて、サービス提供元事業者は、ICカードのオペレーティング・システムに対して

、デフォルトのエリアID$_i$の変更要求を行なう。このシステム・コード変更要求は、デフォルトのエリアIDと、エリアID変更パッケージを引数として行なわれる。エリアID変更パッケージは新規の発行者鍵K_{li}'で暗号化されているので、第3者からは改竄されない。

[0129] エリアID変更要求がICカードのオペレーティング・システムに届くと、引数に含まれるエリアIDに基づいて、エリアID変更パッケージが当該サービス提供元事業者のファイル・システムへ渡され、そのカード発行者鍵K_{li}'で解読され、エリアID変更パッケージが取り出される。そして、ファイル・システムのデフォルトのエリアID$_i$がエリアID$_i$'に変更されると、そのステータスが要求元であるサービス提供元事業者に返される。

[0130] このように新規のサービス提供元事業者は、自己のファイル・システムに対しセキュアな発行者鍵K_{li}'とシステム・コードSC_i'を設定することにより、元のICカード発行者とは独立してセキュリティに関する脅威を分析、管理、並びに運用することができるようになる。

[0131] 上述したように、本実施形態では、ICカード上のメモリ領域は、複数のファイル・システムに分割されている(図15を参照のこと)。そして、ファイル・システム毎にシステム・コードSCとエリアIDが設定されるとともに、当該領域を使用するサービス提供元事業者(元のカード発行者を含む)の発行者鍵K_{li}で相互認証を行なうことができる。これによって、ファイル・システムが割り振られたサービス提供元事業者は、元のカード発行者や分割技術者とは独立して、自己のファイル・システムのセキュリティに関する脅威を分析、管理、並びに運用することができる。

[0132] また、サービス提供元事業者が自己のファイル・システムへアクセスする際には、基本的には、エリアIDの要求と、相互認証という手続きを経て行なわれる。まず、自身が判っているシステム・コードを引数にしてファイル・システムに対するポーリングを行なうことによって、該当するファイル・システムのメモリ領域上でのエリアIDを取得することができる。次いで、このエリアIDと発行者鍵K_lを用いて相互認証を行なう。そして、相互認証が成功裏に終わると、ファイル・システムへのアクセスが許可される。

[0133] また、各サービス提供元事業者(元のカード発行者を含む)は、要求コマンド(例えばリード要求やライト要求、データ消去要求、エリア/サービス登録(後述)など)を、

事業者自身と該当するファイル・システムに固有の発行者鍵K_Iを用いてパッケージ化して暗号化通信により行なわれるので（図16を参照のこと）、他のファイル・システムが無関係のデータを取り込んだり、第3者がファイル・システムへ無断で読み書きしたりすることはできない。

[0134] ICカードのメモリ領域は、分割操作を繰り返すことにより、図15に示すように複数のファイル・システムが共存する構造となる。元のカード発行者、並びにカード発行者の許可によりICカード上で自己のファイル・システムを取得したサービス提供元事業者は、それぞれ自己のファイル・システムを利用して、エリアやサービスを配設し（後述）、自身の事業展開に利用することができる。

[0135] 以下では、1つのファイル・システム内での運用形態について説明する。基本的には、どのファイル・システムにおいても同様の動作が実現されるものとする。また、ファイル・システムの操作を行なうためには、ポーリングによるエリアIDの要求と、相互認証という手続き（前述）を経ていることを前提とする。

[0136] ファイル・システム内には、電子決済を始めとする外部との電子的な価値情報のやり取りなど、1以上のアプリケーションが割り当てられている。アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ。また、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

[0137] ユーザがアクセス権を持つかどうかに応じてアプリケーションの利用すなわちサービスの起動を制限するために、アプリケーションに対して暗証コードすなわちPINを割り当て、サービス実行時にPINの照合処理を行なうようになっている。また、サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

[0138] 本実施形態では、ICカード内のメモリ領域に設定されているそれぞれのファイル・システムに対して、「ディレクトリ」に類似する階層構造を導入する。そして、メモリ領域に割り当てられた各アプリケーションを、所望の階層の「エリア」に登録することができる。

[0139] 例えば、一連のトランザクションに使用される複数のアプリケーション、あるいは関連性の深いアプリケーション同士を同じエリア内のサービス・メモリ領域として登録する(さらには、関連性の深いエリア同士を同じ親エリアに登録する)ことによって、メモリ領域のアプリケーションやエリアの配置が整然とし、ユーザにとってはアプリケーションの分類・整理が効率化する。

[0140] また、ファイル・システムへのアクセス権を階層的に制御するために、アプリケーション毎にPINを設定できる以外に、各エリアに対してもPINを設定することができるようにしている。例えば、あるエリアに該当するPINを入力することにより、照合処理並びに相互認証処理を経て、エリア内のすべてのアプリケーション(並びにサブエリア)へのアクセス権を与えるようにすることもできる。したがって、該当するエリアに対するPINの入力を1回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。

[0141] さらに、あるサービス・メモリ領域に対するアクセス権限が単一でないことを許容し、それぞれのアクセス権限毎、すなわちサービス・メモリ領域において実行するサービスの内容毎に、暗証コードを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のPINが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のPINが設定される。また、あるメモリ領域に対する読み出しについてはPINの入力が必要でないが、書き込む場合にはPINの入力を必須とさせることが可能である。

[0142] 図17には、ファイル・システム内のデータ構造例を模式的に示している。図示の例では、ファイル・システムが持つ記憶空間には、「ディレクトリ」に類似する階層構造が導入されている。すなわち、メモリ領域に割り当てられた各アプリケーションを、所望の階層エリアにサービス・メモリ領域として登録することができる。例えば、一連のトランザクションに使用されるアプリケーションなど、関連性の深いアプリケーション同士を同じエリアに登録する(さらには、関連性の深いエリア同士を同じ親エリアに登録する)ことができる。

[0143] また、ファイル・システム内に割り当てられたアプリケーション（すなわちサービス・メモリ領域）並びにエリアは暗証コード定義ブロックを備えている。したがって、アプリケーション毎に、あるいはエリア毎にPINを設定することができる。また、ファイル・システムに対するアクセス権は、アプリケーション単位で行なうとともに、並びにエリア単位で行なうことができる。

[0144] さらに、あるサービス・メモリ領域に対するアクセス権限が単一でなく、実行するサービスの内容毎に、PINを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のPINが設定され、また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のPINが設定される。

[0145] 照合部は、例えば電磁誘導作用に基づく非接触近距離通信又はUART48やI^2C 49などのプロトコル・インターフェースを介して送られてくるPINを、各アプリケーション又はディレクトリに割り当てられたエリア又はサービス・メモリ領域に設定されている暗証コードと照合して、一致するメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、プロトコル・インターフェースを介して読み書きが可能となる。

[0146] このようにファイル・システム内には、アプリケーションに割り当てられたさまざまなサービス・メモリ領域が割り当てられており、各サービス・メモリ領域に対して適用可能な1以上のサービスが設けられている。本実施形態では、エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、アプリケーションに適用されるサービスの種類毎にPINを設定して、サービス単位でアクセス制限を行なうことができる。

[0147] 図18には、ファイル・システムの基本構成を示している。図17を参照しながら既に説明したように、ファイル・システムに対して、「ディレクトリ」に類似する階層構造が導入され、所望の階層のエリアに、アプリケーションに割り当てられたサービス・メモリ領域を登録することができる。図18に示す例では、エリア0000定義ブロックで定義されるエリア0000内に、1つのサービス・メモリ領域が登録されている。

[0148] 図示のサービス・メモリ領域は、1以上のユーザ・ブロックで構成される。ユーザ・ブロックはアクセス動作が保証されているデータ最小単位のことである。このサービス・メ

モリ領域に対しては、サービス0108定義ブロックで定義されている1つのサービスすなわちサービス0108が適用可能である。

[0149] エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、サービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。アクセス制限の対象となるサービスに関する暗証コード設定情報は、暗証コード専用のサービス(すなわち「暗証コード・サービス」)として定義される。図18に示す例では、サービス0108に関する暗証コードが暗証コード・サービス0128定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

[0150] サービス0108に対する暗証コード・サービスが有効になっている場合、サービス0108を起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なう前に、暗証コード・サービス0128を使用した暗証コードの照合が必要となる。具体的には、暗号化あり読み書き(Read／Write)コマンドを使用する場合は、相互認証前にサービス0108に対する暗証コードすなわちPINの照合を行なう。

[0151] また、アプリケーションに割り当てられたサービス・メモリ領域を所望の階層のエリアに登録するとともに、エリアを階層化する(関連性の深いエリア同士を同じ親エリアに登録する)ことができる。この場合、エリア毎にPINを設定することにより、エリアをアクセス制限の単位とすることができる。図19には、ICカード50のメモリ空間においてエリアが階層化されている様子を示している。同図に示す例では、エリア0000定義ブロックで定義されているエリア0000内に、エリア1000定義ブロックで定義されている別のエリア1000が登録されている。

[0152] 図19に示す例では、さらにエリア1000内には、2つのサービス・メモリ領域が登録されている。一方のサービス・メモリ領域に対しては、サービス1108定義ブロックで定義されているサービス1108と、サービス110B定義ブロックで定義されているサービス110Bが適用可能である。このように、1つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義することを、本明細書中では「オーバーラップ・サービス」と呼ぶ。オーバーラップ・サービスにおいては、同じサービス・エリアに対して、入力したPINに応じて異なるサービスが適用されることになる。また、他方のサー

ビス・メモリ領域に対しては、サービス110C定義ブロックで定義されているサービス110Cが適用可能である。

[0153] 各サービス・メモリ領域に設定されているサービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことができる。勿論、図18を参照しながら説明したように、サービス毎に暗証コード・サービスを定義することができる。この場合、サービスに対する暗証コード・サービスが有効になっているときには、暗証コード・サービスを使用したPINの照合を行なってからサービスの起動が許可される。

[0154] また、複数のサービスに対して共通のPINを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。

[0155] 図19に示す例では、エリア1000に関する暗証コードが、暗証コード・サービス1020定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

[0156] エリア1000に対する暗証コード・サービスが有効(後述)になっている場合、暗証コード・サービス1020を使用した暗証コードの照合を行なった後に、エリア1000内の各サービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことが可能となる。

[0157] ここで、エリア1000内のサービスに暗証コード・サービスが適用されており且つこれが有効となっている場合には、さらにその暗証コード・サービスを使用した暗証コードの照合を経てからでないと、そのユーザ・ブロックに読み出し又は書き込み動作を行なうことはできない。

[0158] 図18及び図19に例示したように、暗証コード照合の対象となるエリアやサービスに対応する暗証コード・サービスは一意に与えられる。

[0159] 図20には、ファイル・システム内にエリアやサービスを登録するための手順をフローチャートの形式で示している。

[0160] まず、メモリ空間にエリアが定義される(ステップS1)。

[0161] 次いで、サービスの登録サービス・コマンドを使用して、エリア内にアプリケーションに対してサービス・メモリ領域を割り当てるとともに、このサービス・メモリ領域に適用さ

れるサービスを定義する(ステップS2)。登録サービス・コマンドでは、サービス・メモリ領域のユーザ・ブロック数を指定する。エリア内で複数のアプリケーションを割り当てたい場合には、当該処理ステップを繰り返し実行する。

[0162] エリア内で定義したサービスに対して暗証コードを適用したい場合には、サービスの登録サービス・コマンドを使用して、暗証コード・サービスの登録を行なう(ステップS3)。

[0163] 暗証コード・サービスの登録は、通常のサービスと同様の登録サービス・コマンドを使用して行なう。但し、暗証コード・サービスの登録は、暗証コード照合の対象となるエリアやサービスが既にファイル・システムに登録済みであることが条件となる。すなわち、PIN照合の対象となるエリアやサービスがない場合は、暗証コード・サービスの登録サービス実行時にエラーとなる。また、暗証コード・サービスは、通常のサービスのユーザ・ブロックに相当する暗証コード・サービス・データ・ブロックが1ブロックしか存在しないので、サービス登録時に登録サービス・コマンドで指定ユーザ・ブロック数を1以外の値に設定するとエラーとなる。

[0164] さらに、エリア内で定義されたすべてのサービスに対して共通の暗証コードを設定したい場合には、サービスの登録サービス・コマンドを使用して、このエリアに対して共通の暗証コード・サービスの登録を行なう(ステップS4)。

[0165] なお、ステップS3とステップS4の実行順序は逆であってもよい。

[0166] さらに、1つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義したい場合には、サービスの登録サービス・コマンドを使用して、オーバーラップ・サービス(図19を参照のこと)を登録する(ステップS5)。

[0167] そして、オーバーラップ・サービスに対して暗証コードを適用したい場合には、サービスの登録サービス・コマンドを使用して、暗証コード・サービスの登録を行なう(ステップS6)。

[0168] 図18に示した例では、ルートのエリア0000内にサービス・メモリ領域の割り当て並びにこれに適用するサービス0108が登録された後、サービス0108に適用される暗証コード・サービスが登録される。

[0169] また、図19に示した例では、ルートのエリア0000下のエリア1000内で、2つのサー

ビス・メモリ領域が割り当てられるとともに、それぞれに適用されるサービス1108、サービス110Cが登録される。また、一方のサービス・メモリには、他のサービス110Bがオーバーラップ・サービスとして登録される。図示しないが、これらに暗証コードを適用したい場合には、別途、暗証コード・サービスの登録が行なわれる。そして、登録されたサービス1108，110B，110Cに対して共通の暗証コードを設定したい場合には、エリア1000に対して共通の暗証コード・サービスを登録する。

[0170] サービス提供元事業者（元のカード発行者を含む）は、自分に割り振られたファイル・システム内にエリアやサービスを登録したい場合には、ICカードの実行環境を提供するオペレーティング・システムに対してエリア登録要求やサービス登録要求をおこなう。これらの登録要求コマンドは事業者自身と該当するファイル・システムに固有の発行者鍵K_Iを用いてパッケージ化して暗号化通信により行なわれるので（図16を参照のこと）、他のファイル・システムが無関係のデータを取り込んだり、第3者がファイル・システムへ無断で読み書きしたりすることはできない。

[0171] 図21には、図20に示した処理手順のステップS1において実行される、サービス提供元事業者（元のカード発行者を含む）が自己のファイル・システム内にエリア登録を行なう手続きを示している。但し、サービス提供元事業者とICカード間の通信は、電磁誘導作用に基づく非接触近距離通信インターフェースを利用しても、あるいはUART48やI^2C49などの有線インターフェースを利用して行なう。

[0172] サービス提供元事業者は、ICカードの実行環境であるオペレーティング・システムに対しポーリングして、ファイル・システムのシステム・コードSCを引数にしたファイル・システムのエリアID要求を行なう。

[0173] この要求メッセージをトリガにして、サービス提供元事業者と、ICカードの実行環境であるオペレーティング・システムの間で、複数往復にまたがる通信動作で構成される相互認証手続きを経て、要求に対する戻り値として、エリアIDがサービス提供元事業者へ返される。なお、相互認証手続きの構成についてはICカードの仕様毎に相違し、本発明の要旨には直接関連しないので、ここでは詳細な説明を省略する。

[0174] この認証手続きに続いて、サービス提供元事業者は、ICカードのオペレーティング・システムに対して、ファイル・システム内へのエリア登録要求を行なう。このエリア登

録要求は、エリアIDと、エリア登録要求パッケージを引数として行なわれる。エリア登録要求パッケージは当該サービス提供元事業者の発行者鍵K_Iで暗号化されているので、第3者からは改竄されない。

[0175] エリア登録要求がICカードのオペレーティング・システムに届くと、引数に含まれるエリアIDに基づいて、エリア登録要求パッケージが当該サービス提供元事業者のファイル・システムへ渡され、その発行者鍵K_Iで解読され、エリア登録要求パッケージが取り出される。そして、パッケージ内で要求されているエリアがファイル・システム内に登録されると、そのステータスが要求元であるサービス提供元事業者に返される。

[0176] また、図22には、図20に示した処理手順のステップS2において実行される、サービス提供元事業者（元のカード発行者を含む）が自己のファイル・システム内（若しくはファイル・システムに登録されている特定のエリア）にサービス登録を行なう手続きを示している。但し、サービス提供元事業者とICカード間の通信は、電磁誘導作用に基づく非接触近距離通信インターフェースを利用しても、あるいはUART48やI^2C49などの有線インターフェースを利用して行なう。

[0177] サービス提供元事業者は、ICカードの実行環境であるオペレーティング・システムに対しポーリングして、ファイル・システムのシステム・コードSCを引数にしたファイル・システムのエリアID要求を行なう。

[0178] この要求メッセージをトリガにして、サービス提供元事業者と、ICカードの実行環境であるオペレーティング・システムの間で、複数往復にまたがる通信動作で構成される相互認証手続きを経て、要求に対する戻り値として、エリアIDがサービス提供元事業者へ返される。なお、相互認証手続きの構成についてはICカードの仕様毎に相違し、本発明の要旨には直接関連しないので、ここでは詳細な説明を省略する。

[0179] この認証手続きに続いて、サービス提供元事業者は、ICカードのオペレーティング・システムに対して、ファイル・システム内（若しくはファイル・システムに登録されている特定のエリア）へのサービス登録要求を行なう。このサービス登録要求は、エリアIDと、サービス登録要求パッケージを引数として行なわれる。サービス登録要求パッケージは当該サービス提供元事業者の発行者鍵K_Iで暗号化されているので、第3者からは改竄されない。

[0180] サービス登録要求がICカードのオペレーティング・システムに届くと、引数に含まれるエリアIDに基づいて、サービス登録要求パッケージが当該サービス提供元事業者のファイル・システムへ渡され、その発行者鍵K_Iで解読され、サービス登録要求パッケージが取り出される。そして、パッケージ内で要求されているサービスがファイル・システム内（若しくはファイル・システムに登録されている特定のエリア）に登録されると、そのステータスが要求元であるサービス提供元事業者に返される。

[0181] 図18及び図19に例示したように、ファイル・システム内に登録されたエリアやサービスに対してPINを適用して、エリア単位、あるいはサービス単位でアクセス制御を行なうことができる。また、1つのサービス・メモリ領域に対して複数のサービス（オーバーラップ・サービス）を登録することができるが、サービス毎にPINを適用することで、同じサービス・メモリ領域に対して複数のアクセス方法を定義することができる。

[0182] 但し、本実施形態では、ファイル・アクセスへアクセスする際、発行者鍵を用いた相互認証処理（前述）は必須であるが、PIN照合処理は任意である。すなわち、サービス又はエリアに対する暗証コード・サービスが有効になっている場合にのみ、サービスの起動又はエリアへのアクセスを行なう前に、暗証コードの照合が要求され、暗証コード・サービスが無効にされている場合には、PINの照合は要求されない。

[0183] PINの適用内容は、暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックに記述されている。図23には、暗証コード・サービス・データ・ブロックのデータ構造を模式的に示している。同図に示すように、暗証コード定義領域は、暗証番号領域と、入力失敗回数記憶領域と、最大許容入力失敗回数設定領域と、暗証番号使用選択領域と、アクセス許可フラグとで構成されている。

[0184] ユーザが入力したPINが一致した場合にのみ、該当するサービス又はエリアの暗証コード・サービス・データ・ブロック内のアクセス許可フラグを立てて、其処へのアクセスを許可する。

[0185] アクセス許可フラグは、該当するアプリケーション又はディレクトリのアクセス可否状態を示すためのフラグであり、アクセス許可フラグが設定されたサービス又はエリアはアクセス許可状態である。PINが設定されたサービスやエリアのアクセス許可フラグは、デフォルトではアクセス不可状態であり、PIN照合処理及びファイル・システムの

発行者鍵を用いた相互認証処理に成功した後、アクセス許可フラグが設定されて、アクセス許可状態に転じる。また、アクセス許可フラグを設定し続けると、ICカードが紛失した場合や盗難に遭った場合にサービスやエリアの無断使用・不正使用によりユーザが損害を被るおそれがある。このため、ICカードは、例えば電磁波が途絶えたことに応答してアクセス許可状態を自動的にアクセス不可にする機構を備えていてもよい。

[0186] また、誤ったPINが入力された場合には、その都度、入力失敗回数記憶領域の記録を更新する。そして、入力失敗回数が最大許容入力失敗回数設定領域に設定された最大許容入力失敗回数に到達した場合には、該当するサービスの起動又はエリアに対するアクセスを禁止する。

[0187] 一般には、この入力失敗回数は、一度入力に成功したらクリアするべきものである。このようにして悪意あるユーザがしらみつぶしに暗証コードを調べることを防止する。また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、ICカードを管理する管理者(例えば分割技術管理者や元のカード発行者)のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば後述するような秘密鍵による認証を使用することもできる。

[0188] 図24には、ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順をフローチャートの形式で示している。

[0189] ユーザから暗証コードを入力すると(ステップS11)、各暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックにアクセスして、暗証コードが一致するか否かを判別する(ステップS12)。

[0190] 暗証コード・サービス・データ・ブロックのPINがユーザ入力されたPINと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、対応するサービス又はエリアをアクセス可能状態にする(ステップS13)。

[0191] 例えば、ICチップをリーダ/ライタにかざして、リーダ/ライタに接続されている外部機器(図示しない)のユーザ・インターフェースを用いて入力されたPINを、電磁誘導作用に基づく非接触近距離通信インターフェースでICカードに送信することができる。

[0192] 図24に示すようにPINを用いてアプリケーションやディレクトリへのアクセス権を制御する場合、悪意のあるユーザはしらみつぶしにPINを調べることにより、セキュリティの壁が破られる可能性がある(特に桁数の少ない暗証コードを用いる場合)。このため、本実施形態では、暗証コード定義領域において、最大許容入力回数を設定して、入力失敗回数が最大許容入力回数に到達したアプリケーション又はディレクトリをアクセス不可状態に設定することで、アクセス制御を行なうようにしている。

[0193] 図25には、PINの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順をフローチャートの形式で示している。

[0194] ユーザからPINを入力すると(ステップS21)、各暗証コード・サービス定義ブロックにアクセスして、PINが一致するか否かを判別する(ステップS22)。

[0195] ユーザ入力されたPINが暗証コード・サービス定義ブロックのPINと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、該当するサービス又はエリアをアクセス可能状態にする(ステップS23)。

[0196] 他方、ユーザ入力されたPINがいずれの暗証コード・サービス定義ブロックのPINとも一致しない場合には、暗証コード定義領域内の入力失敗回数を更新する(ステップS24)。また、ユーザ入力されたPINがいずれの暗証コード・サービス定義ブロックのPINと一致し、照合に成功した場合には、入力失敗回数を0にクリアする。

[0197] そして、ステップS25では、更新された入力失敗回数が、暗証コード定義領域内で設定されている最大許容入力回数に到達したか否かを判断する(ステップS25)。

[0198] もし、入力失敗回数が最大許容入力回数に到達してしまったならば、その暗証コード定義領域内のアクセス許可フラグの設定を解除して、該当するサービス又はエリアをアクセス不可状態にする(ステップS26)。この結果、悪意のあるユーザがしらみつぶしにPINを調べる行為を取り締まることができる。

[0199] また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、ICカードを管理する管理者(例えば、分割技術管理者、または元のカード発行者)のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば秘密鍵による認証を使用することもできる。

産業上の利用可能性

[0200] 以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

[0201] 本明細書では、ICカードに内蔵されているメモリ領域についての情報管理方法を例にとって本発明の一実施形態について説明してきたが、本発明の要旨はこれに限定されるものではなく、ICカード以外の機器に内蔵されているメモリの管理にも同様に適用することができる。

[0202] 要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、請求の範囲の記載を参酌すべきである。

図面の簡単な説明

[0203] [図1]図1は、電磁誘導に基づくカード読み書き装置とICカードとの無線通信の仕組みを概念的に示した図である。

[図2]図2は、カード読み書き装置とICカードからなる系を1個のトランスとして捉えてモデル化した図である。

[図3]図3は、本発明の実施形態に係るデータ通信装置のハードウェア構成を示した図である。

[図4]本発明の一実施形態に係るICカードにおけるメモリ領域の制御システム構成を模式的に示した図である。

[図5]図5は、ICカードを用いたサービス提供システムの全体的構成を模式的に示した図である。

[図6]図6は、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示した図である。

[図7]図7は、カード発行者が自らのファイル・システムの空き領域の内で、ある範囲のメモリを領域管理者に貸与(又は譲渡)することが許可できることを示した図である。

[図8]図8は、他のサービス提供元事業者が、カード発行者から許可された領域においてメモリ領域を分割し、新たなファイル・システムを生成した状態を示した図である。

[図9]図9は、共通領域管理者が、カード発行者から許可された領域において、共通

領域のシステム・コードSC0でメモリを分割した状態を示した図である。

[図10]図10は、ファイル・システムを分割する際の事前処理を説明するための図である。

[図11]図11は、カード発行者がICカードに対してポーリングを行なう手続きを示したシーケンス図である。

[図12]図12は、カード発行者がICカードに対して分割要求を行なう手続きを示したシーケンス図である。

[図13]図13は、ICカード上のメモリ領域が分割され、新たなファイル・システムが生成される様子を示した図である。

[図14]図14は、新規のサービス提供元事業者がICカードのメモリ領域上に自己のファイル・システムを取得した後に行なう、発行者鍵K_{Ii}とシステム・コードSC_iの再設定手続きを示したシーケンス図である

[図15]図15は、分割操作の繰り返しにより、ICカードのメモリ領域上に複数のファイル・システムが共存するメモリ空間の構造を模式的に示した図である。

[図16]図16は、発行者鍵でパッケージ化された要求コマンドの構成を模式的に示した図である。

[図17]図17は、ファイル・システム内のディレクトリ構造例を模式的に示した図である。

[図18]図18は、ファイル・システムの基本構成を示した図である。

[図19]図19は、ICカード50のメモリ空間においてエリアが階層化されている様子を示した図である。

[図20]図20は、ファイル・システム内にエリアやサービスを登録するための手順を示したフローチャートである。

[図21]図21は、サービス提供元事業者(元のカード発行者を含む)が自己のファイル・システム内にエリア登録を行なう手続きを示した図である。

[図22]図22は、サービス提供元事業者(元のカード発行者を含む)が自己のファイル・システム内にサービス登録を行なう手続きを示した図である。

[図23]図23は、暗証コード・サービス・データ・ブロックのデータ構造を模式的に示し

た図である。

[図24]図24は、ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順を示したフローチャートである。

[図25]図25は、PINの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順を示したフローチャートである。

符号の説明

[0204] 11…発行者用通信装置

12…運用者要通信装置

13…製造者用通信装置

14…記憶領域分割装置

15…運用ファイル登録装置

16…ICカード

17…ネットワーク

21…カード発行者

22…カード記憶領域運用者

23…装置製造者

24…カード記憶領域使用者

26…カード所有者

30…カード機能アナログ回路部

31…整流器

32…アンテナ

33…シリアル・レギュレータ

34…搬送波検出器

35…クロック抽出器

36…クロック選択器

37…クロック発振器

38…論理回路

39…電圧検出器

40…データ処理部

41…RAM

42…ROM

43…EEPROM

44…信号処理部

45…CPU

46…データ暗号化エンジン

47…エラー訂正部

48…UARTインターフェース

49…I^2Cインターフェース

50…リーダ／ライタ機能アナログ回路部

51…送信アンプ

52…送信アンテナ

53…受信信号検出器

54…受信アンプ・フィルタ

55…受信アンテナ

100…データ通信装置

請求の範囲

[1] メモリ空間を備え、1以上のファイル・システムに分割して管理するデータ通信装置であって、

分割権限鍵を保持し、前記メモリ空間のファイル・システムへのアクセスを管理する制御手段と、

前記メモリ空間上で第1のサービス提供元に割り当てられ、第1のサービス提供元の発行者鍵を保持する第1のファイル・システムとを備え、

新規のファイル・システムの割り当てを要求する第2のサービス提供元から、前記第2のサービス提供元の発行者鍵を前記分割権限鍵で暗号化してできた分割素パッケージ及び新規のファイル・システムに関する情報を含んだデータ・ブロックを第1のサービス提供元の発行者鍵で暗号化した分割パッケージを受信した場合に、

前記第1のファイル・システムは、受信した分割パッケージを前記第1のサービス提供元の発行者鍵を用いて解読し、分割素パッケージ及び新規のファイル・システムに関する情報を取り出し、

前記制御手段は、前記分割権限鍵を用いて分割素パッケージを解読して前記第2のサービス提供元の発行者鍵を取り出し、新規のファイル・システムに関する情報に従って前記メモリ空間の空き領域を分割して、前記第2のサービス提供元の発行者鍵を保持した第2のファイル・システムに割り当てる、

ことを特徴とするデータ通信装置。

[2] メモリ空間上の各ファイル・システムはエリア識別情報を持ち、

アクセス先となるファイル・システムのエリア識別情報及び該ファイル・システムの発行者鍵で暗号化されたパッケージを引数とする外部アクセスを受信した場合に、前記制御手段は、エリア識別情報を基に該当するファイル・システムへパッケージを渡し、ファイル・システムは自身の発行者鍵でパッケージを解読する、

ことを特徴とする請求項1に記載のデータ通信装置。

[3] メモリ空間上に割り当てられた各ファイル・システムはそれぞれシステム・コードを持ち、

前記制御手段は、分割パッケージの受信に応じて新規のファイル・システムを分割

する際に、発行者鍵、エリア識別情報とともにシステム・コードを該ファイル・システムに設定する、

ことを特徴とする請求項2に記載のデータ通信装置。

[4] ファイル・システム取得後のサービス提供元が自己のシステム・コードを引数にしたエリア識別情報の取得要求を行なった場合に、前記制御手段は、要求されたシステム・コードを基に各ファイル・システムをポーリングして該当するファイル・システムからエリア識別情報を取得し、要求元へ返す、

ことを特徴とする請求項3に記載のデータ通信装置。

[5] 前記制御手段は、ファイル・システム取得後の第2のサービス提供元からの要求に応じて、分割時に前記第2のファイル・システムに設定された発行者鍵又はシステム・コードを書き換える、

ことを特徴とする請求項3に記載のデータ通信装置。

[6] メモリ空間上の各ファイル・システムはエリア識別情報を持ち、

ファイル・システム取得後のサービス提供元から、エリア識別情報及び自己のファイル・システムに対するアクセス要求を自己の発行者鍵で暗号化したパッケージを引数とする外部アクセスを受信した場合に、

前記制御手段は、エリア識別情報を基に該当するファイル・システムへ該暗号化されたパッケージを渡す、

ことを特徴とする請求項1に記載のデータ通信装置。

[7] メモリ空間を備え、1以上のファイル・システムに分割して管理するデータ通信装置におけるメモリ管理方法であって、前記メモリ空間上では、ファイル・システムの分割に関する権限を認証する分割権限鍵と、第1のサービス提供元の発行者鍵によりアクセス権限を認証する第1のファイル・システムが設けられており、

新規のファイル・システムの割り当てを要求する第2のサービス提供元から、前記第2のサービス提供元の発行者鍵を前記分割権限鍵で暗号化した分割素パッケージと新規のファイル・システムに関する情報を含んだデータ・ブロックを第1のサービス提供元の発行者鍵で暗号化した分割パッケージを受信するステップと、

受信した分割パッケージを前記第1のサービス提供元の発行者鍵を用いて解読し

て分割素パッケージ及び新規のファイル・システムに関する情報を取り出すステップと、

前記分割権限鍵を用いて分割素パッケージを解読して前記第2のサービス提供元の発行者鍵を取り出し、新規のファイル・システムに関する情報に従って前記メモリ空間の空き領域を分割して、前記第2のサービス提供元の発行者鍵を保持した第2のファイル・システムに割り当てるステップと、

を具備することを特徴とするメモリ管理方法。

[8] メモリ空間上の各ファイル・システムはエリア識別情報を持ち、外部からのアクセスはアクセス先となるファイル・システムのエリア識別情報及び該ファイル・システムの発行者鍵で暗号化されたパッケージを引数として構成され、

エリア識別情報とパッケージを引数とするファイル・システムへのアクセス要求を受信するステップと、

エリア識別情報を基に該当するファイル・システムへパッケージを渡すステップと、

ファイル・システムが自身の発行者鍵でパッケージを解読するステップと、

をさらに備えることを特徴とする請求項7に記載のデータ通信装置のメモリ管理方法。

[9] メモリ空間上の各ファイル・システムはそれぞれシステム・コードを持ち、

分割パッケージの受信に応じて新規のファイル・システムを分割する際に、発行者鍵、エリア識別情報とともにシステム・コードを該ファイル・システムに設定するステップをさらに備える、

ことを特徴とする請求項8に記載のデータ通信装置のメモリ管理方法。

[10] ファイル・システム取得後のサービス提供元が自己のシステム・コードを引数にしたエリア識別情報の取得要求を行なうステップと、

要求されたシステム・コードを基に各ファイル・システムをポーリングして該当するファイル・システムからエリア識別情報を取得し、要求元へ返すステップと、

をさらに備えることを特徴とする請求項9に記載のデータ通信装置のメモリ管理方法。

[11] 第2のサービス提供元が、前記メモリ空間上に自己のファイル・システムを取得した後、分割時に設定された発行者鍵又はシステム・コードの書き換えを要求するステップと、

該書き換え要求に応じて、分割時に前記第2のファイル・システムに設定された発行者鍵又はシステム・コードを書き換えるステップと、

をさらに備えることを特徴とする請求項9に記載のデータ通信装置のメモリ管理方法。

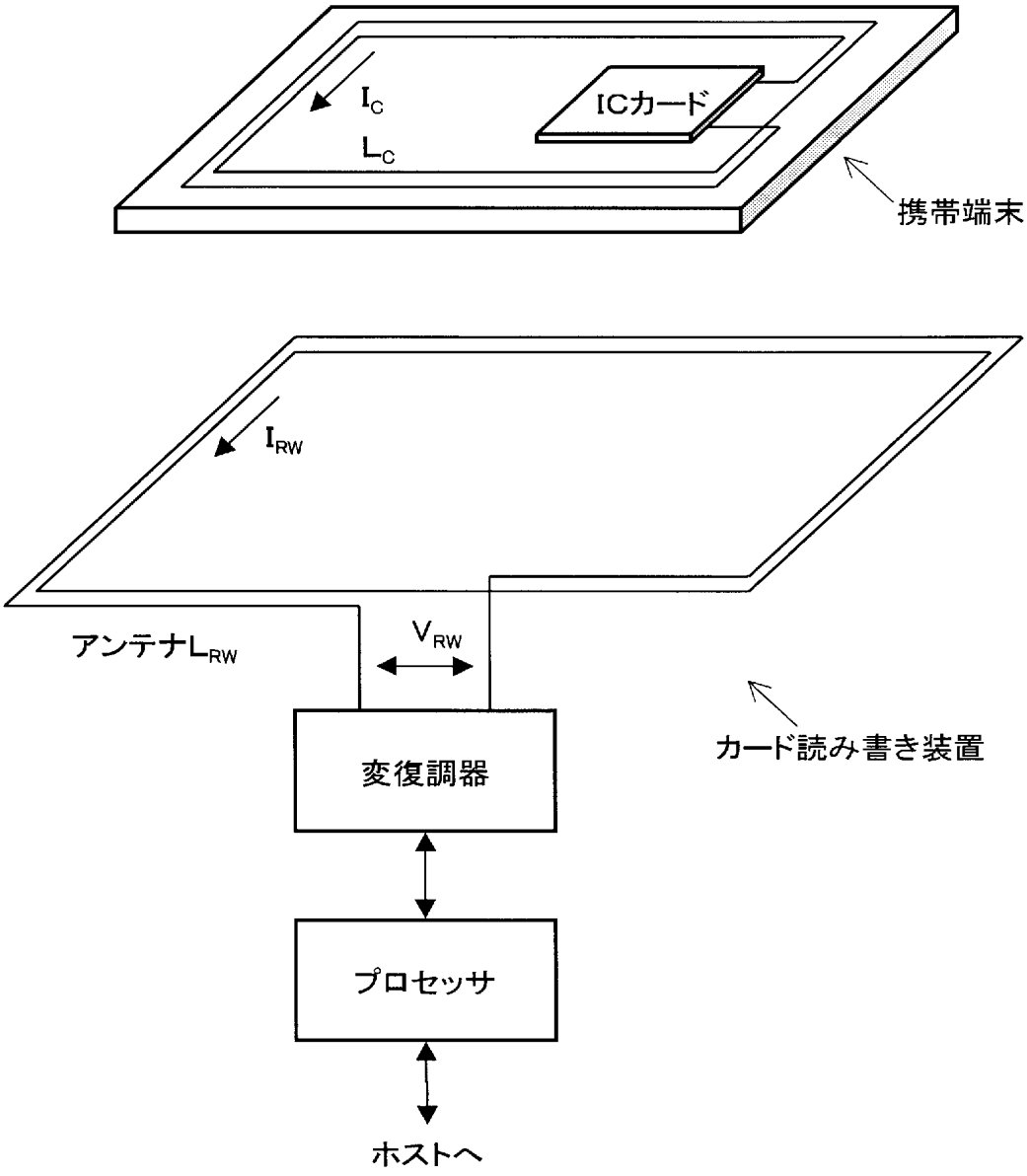
[12] メモリ空間上の各ファイル・システムはエリア識別情報を持ち、

ファイル・システム取得後のサービス提供元がエリア識別情報及び自己のファイル・システムに対するアクセス要求を自己の発行者鍵で暗号化したパッケージを引数とするアクセス要求を受信するステップと、

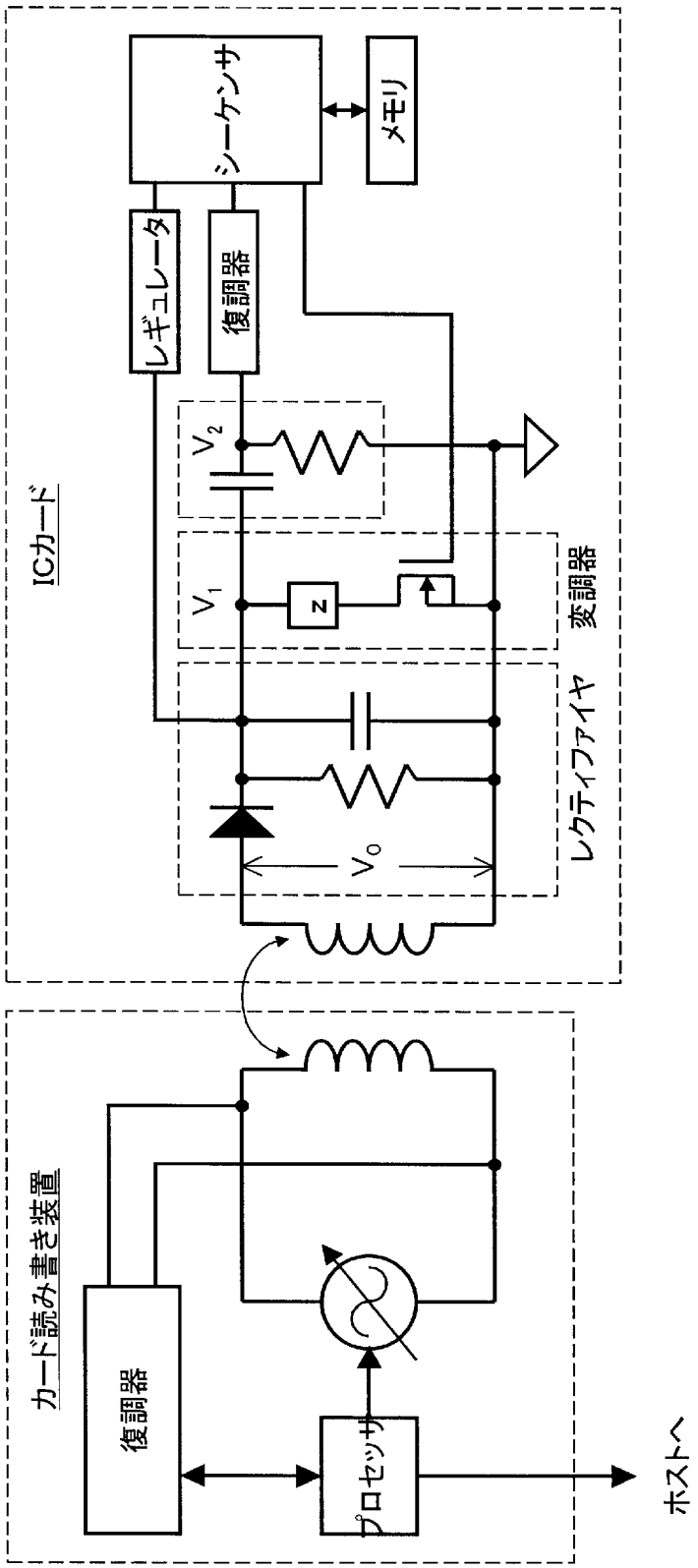
該サービス提供元からのアクセス要求の引数として含まれるエリア識別情報を基に、該当するファイル・システムへパッケージを渡すステップと、

をさらに備えることを特徴とする請求項7に記載のデータ通信装置のメモリ管理方法。

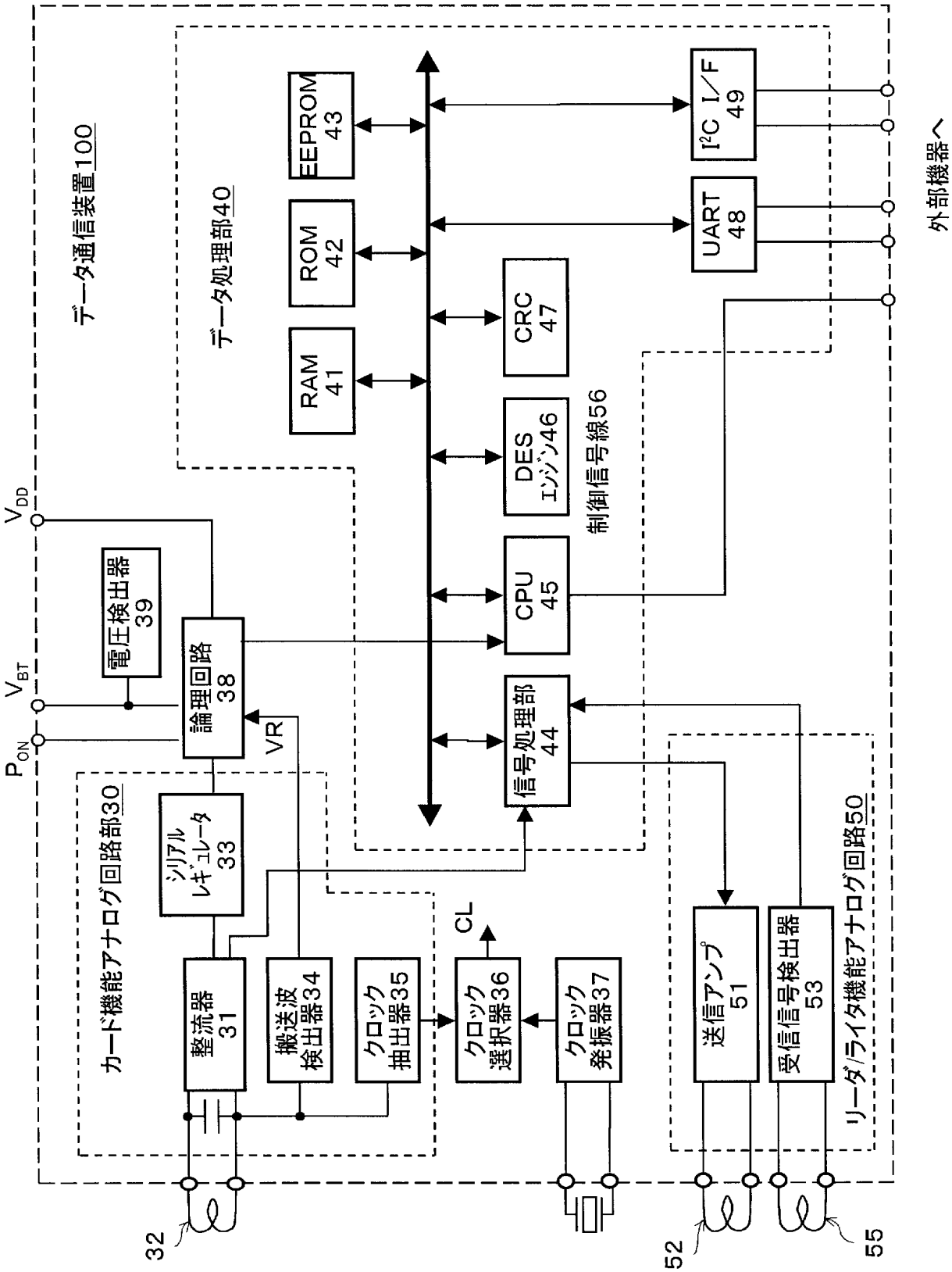
[図1]



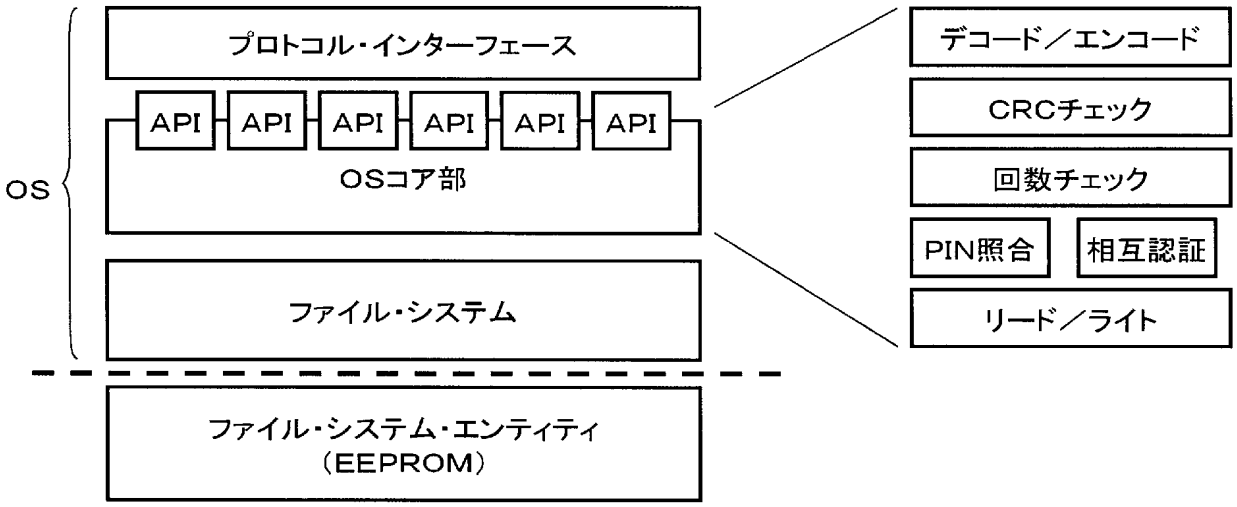
[図2]


ICカード
シーケンサ
メモリ
レギュレータ
復調器
V_2
V_1
Z
変調器
レクティファイヤ
V_o
カード読み書き装置
復調器
プロセッサ
ホストへ

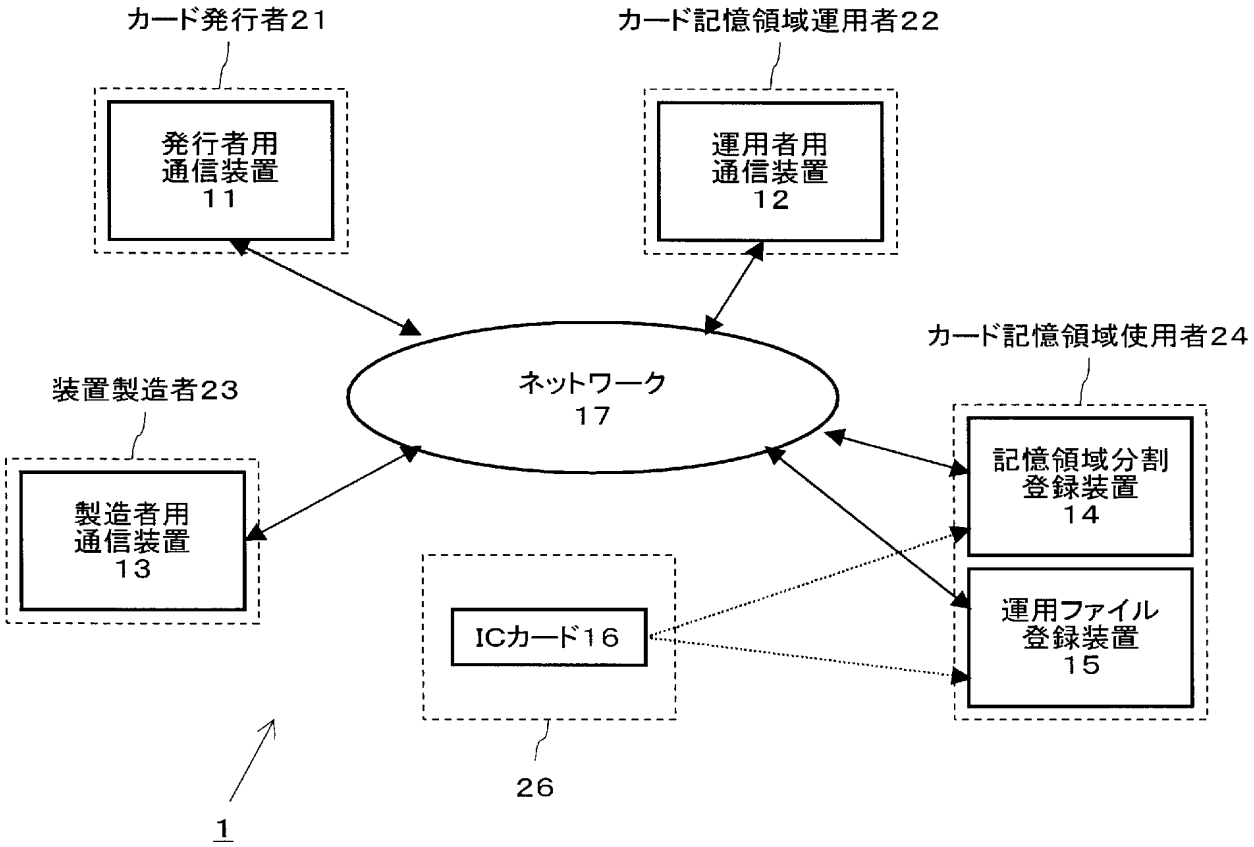
[図3]


データ通信装置100
データ処理部40
EEPROM 43
ROM 42
RAM 41
CRC 47
DES エンジン46
CPU 45
信号処理部 44
I²C I/F 49
UART 48
外部機器へ
制御信号線56
V_{DD}
V_{BT}
P_{ON}
電圧検出器 39
論理回路 38
VR
シリアル レギュレータ 33
カード機能アナログ回路部30
整流器 31
搬送波 検出器34
クロック 抽出器35
クロック 選択器36
クロック 発振器37
CL
送信アンプ 51
受信信号検出器 53
リーダ/ライタ機能アナログ回路50
32
52
55

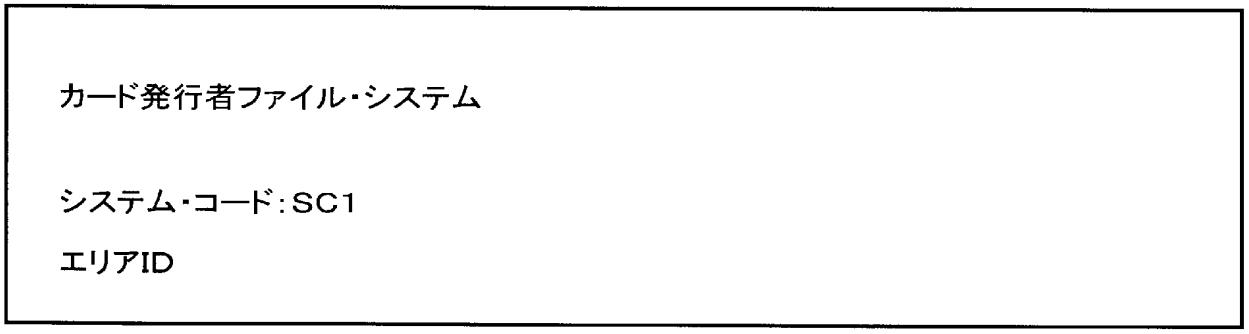
[図4]


OS
プロトコル・インターフェース
API
API
API
API
API
API
OSコア部
ファイル・システム
ファイル・システム・エンティティ
（EEPROM）
デコード／エンコード
CRCチェック
回数チェック
PIN照合
相互認証
リード／ライト

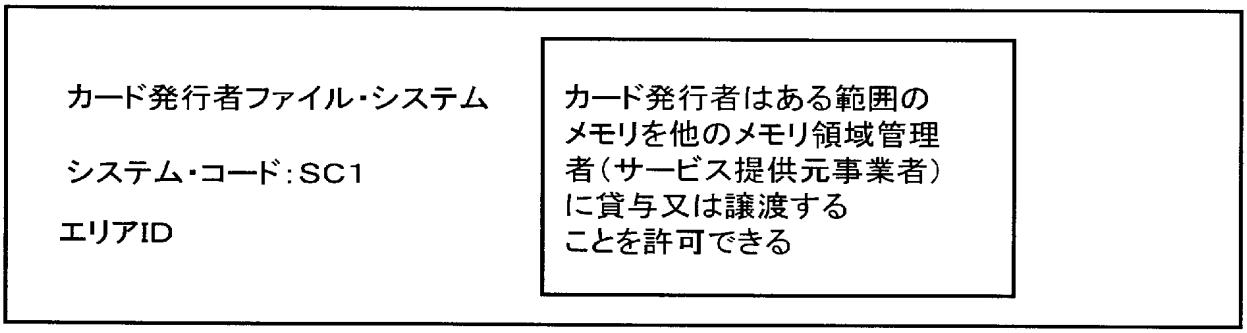
[図5]


カード発行者21
発行者用
通信装置
11
カード記憶領域運用者22
運用者用
通信装置
12
ネットワーク
17
装置製造者23
製造者用
通信装置
13
カード記憶領域使用者24
記憶領域分割
登録装置
14
運用ファイル
登録装置
15
ICカード16
26
1

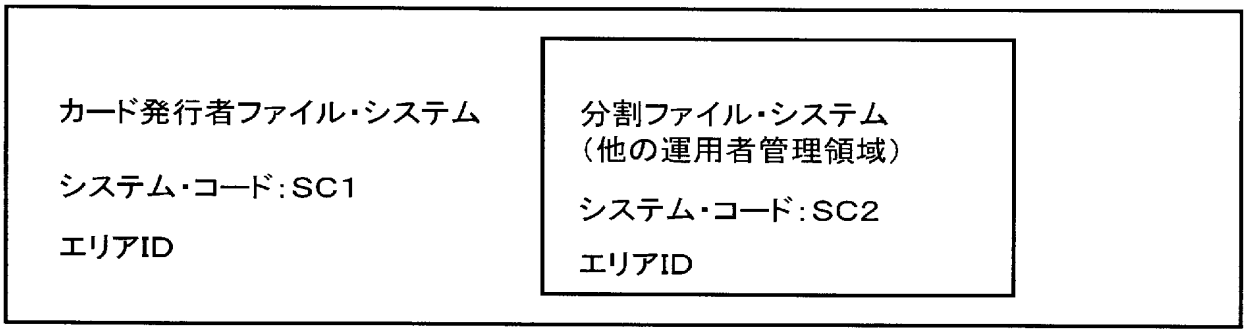
[図6]


カード発行者ファイル・システム
システム・コード：SC1
エリアID

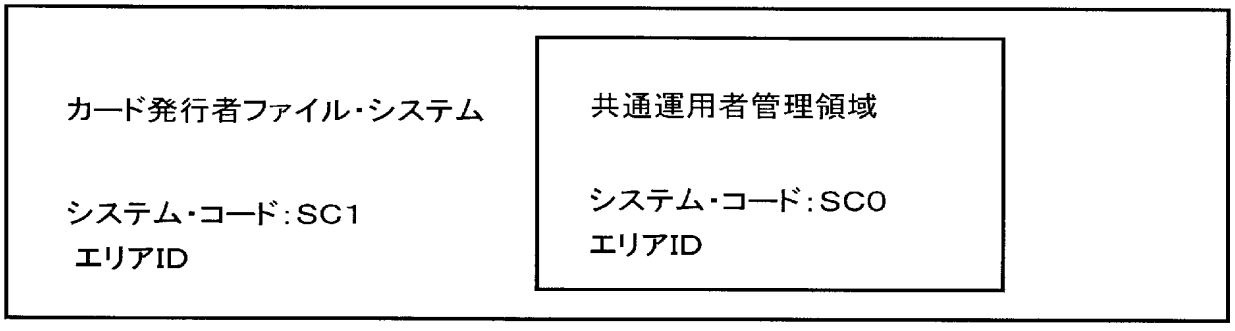
[図7]


カード発行者ファイル・システム
システム・コード：SC1
エリアID
カード発行者はある範囲の
メモリを他のメモリ領域管理
者（サービス提供元事業者）
に貸与又は譲渡する
ことを許可できる

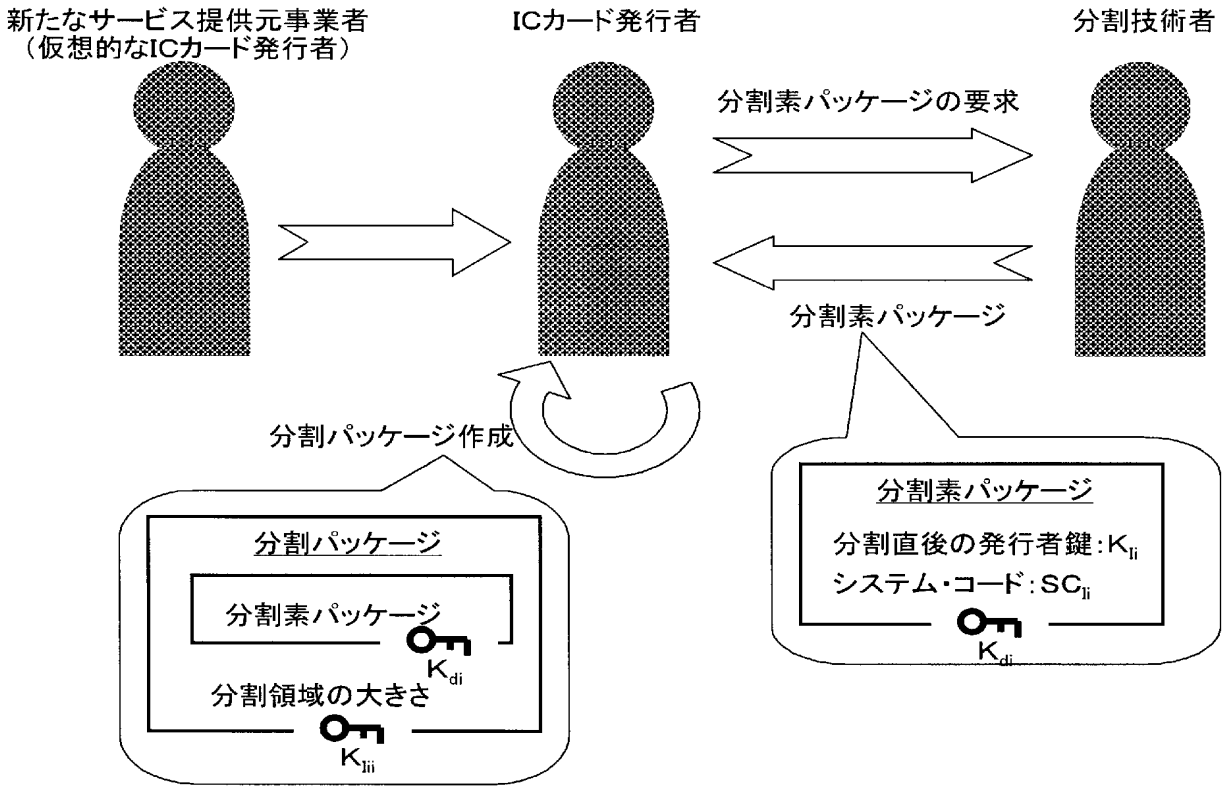
[図8]


カード発行者ファイル・システム
システム・コード：SC1
エリアID
分割ファイル・システム
（他の運用者管理領域）
システム・コード：SC2
エリアID

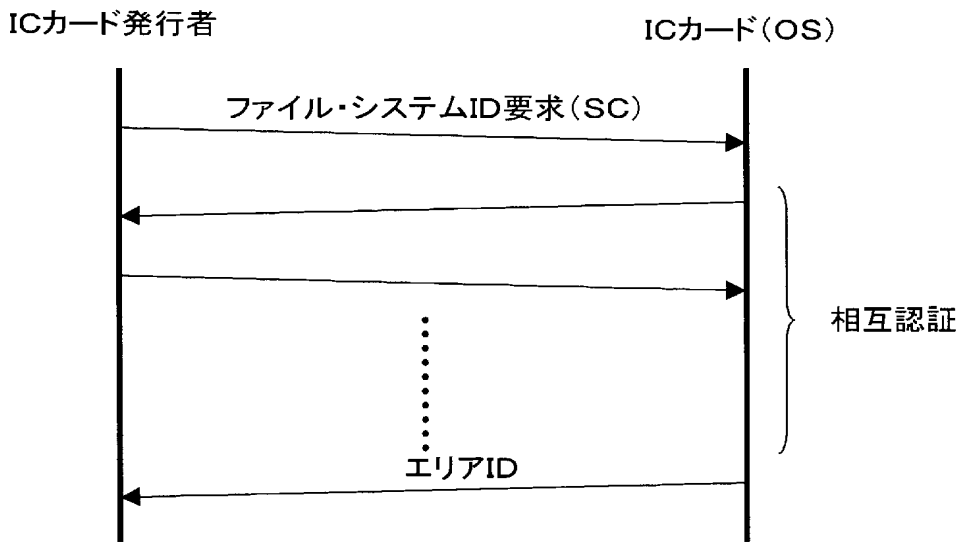
[図9]


カード発行者ファイル・システム
システム・コード：SC1
エリアID
共通運用者管理領域
システム・コード：SC0
エリアID

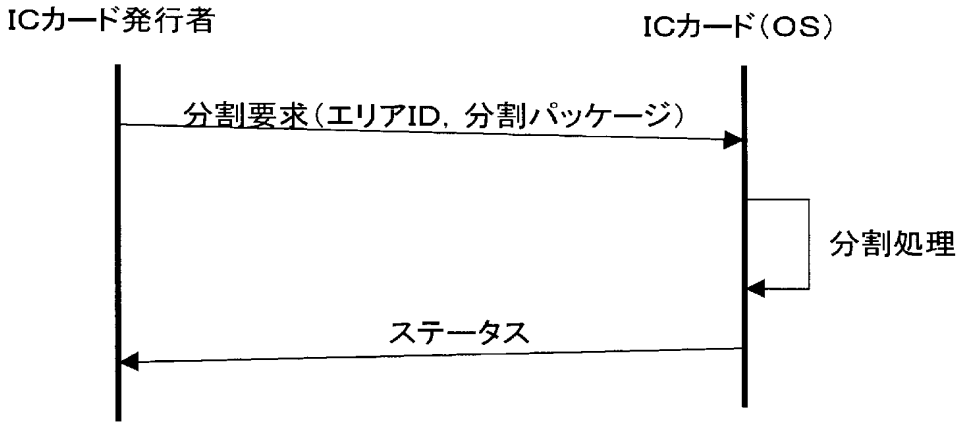
[図10]


新たなサービス提供元事業者
（仮想的なICカード発行者）
ICカード発行者
分割技術者
分割素パッケージの要求
分割素パッケージ
分割パッケージ作成
分割パッケージ
分割素パッケージ
K_{di}
分割領域の大きさ
K_{Iii}
分割素パッケージ
分割直後の発行者鍵：K_{Ii}
システム・コード：SC_{Ii}
K_{di}

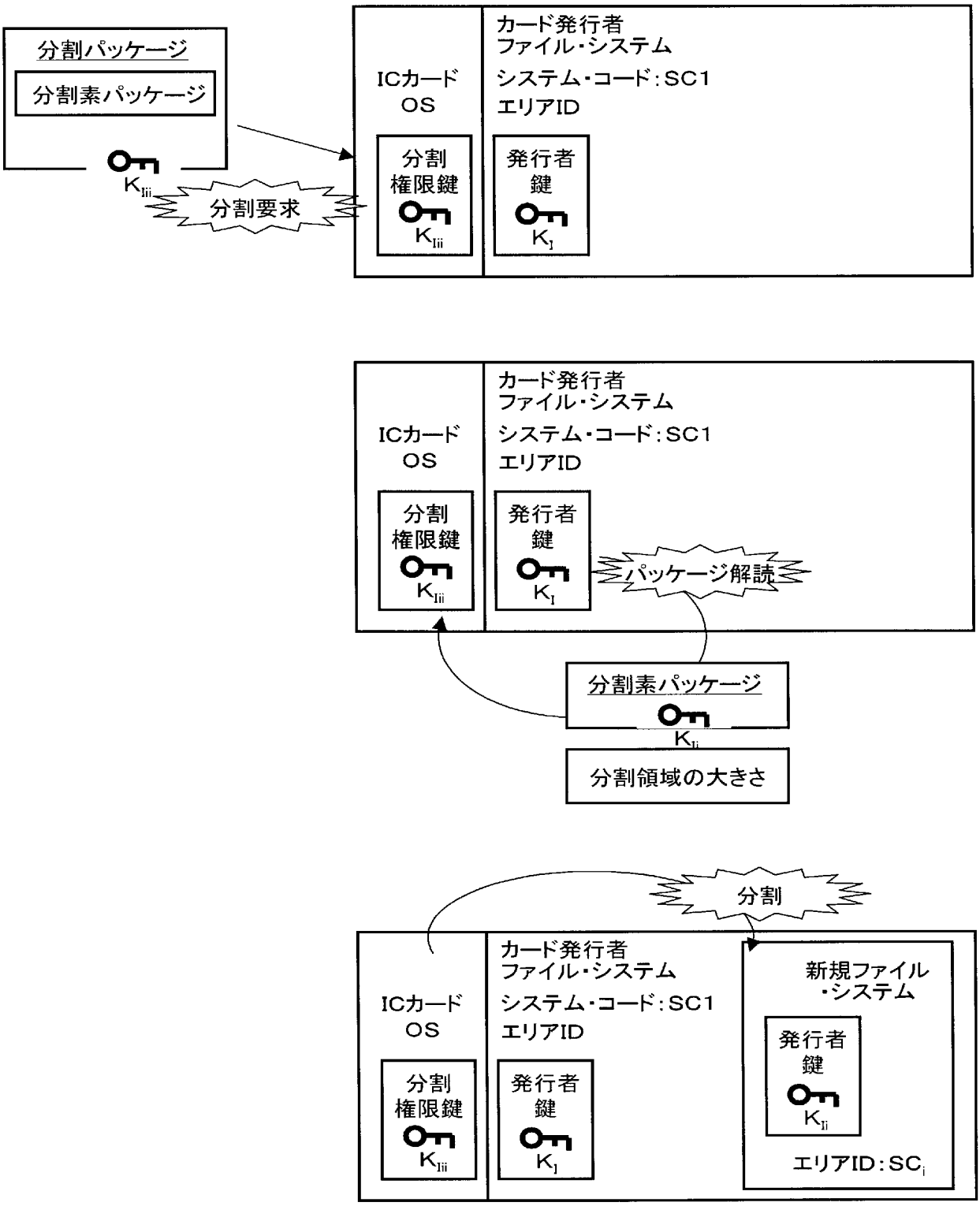
[図11]



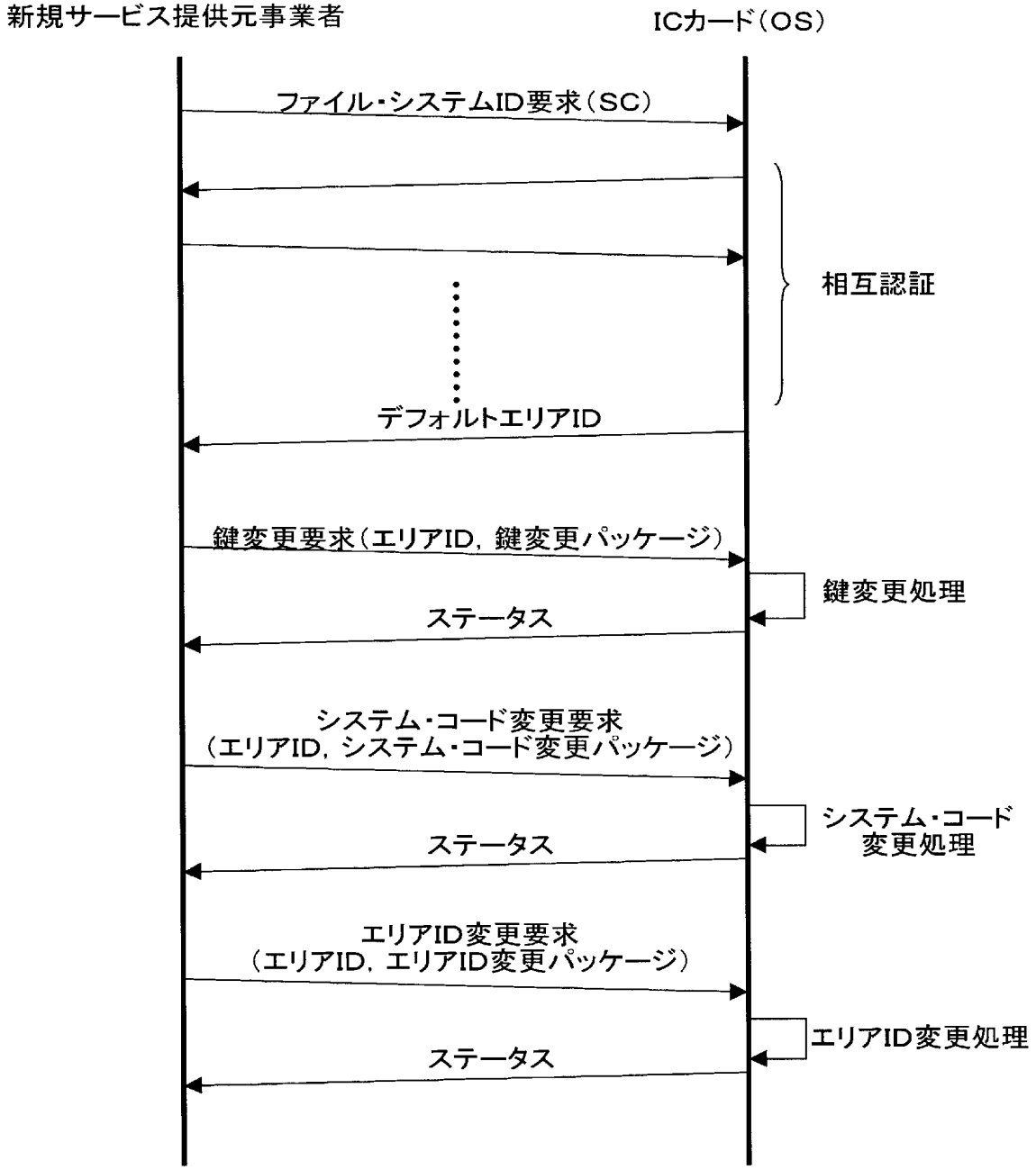
[図12]



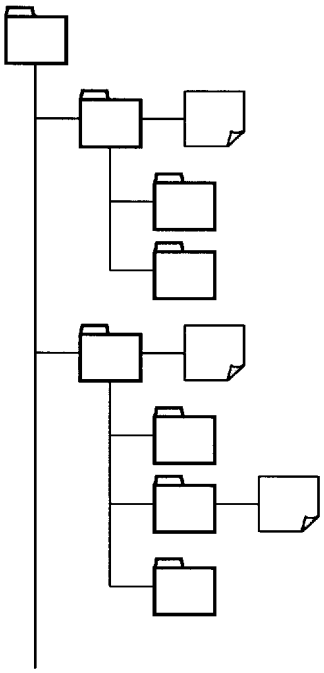
[図13]


分割パッケージ
分割素パッケージ
K_{Iii}
分割要求
ICカード
OS
分割
権限鍵
K_{Iii}
カード発行者
ファイル・システム
システム・コード：SC1
エリアID
発行者
鍵
K_I
パッケージ解読
分割素パッケージ
K_{Ii}
分割領域の大きさ
分割
新規ファイル
・システム
エリアID：SC_i

[図14]

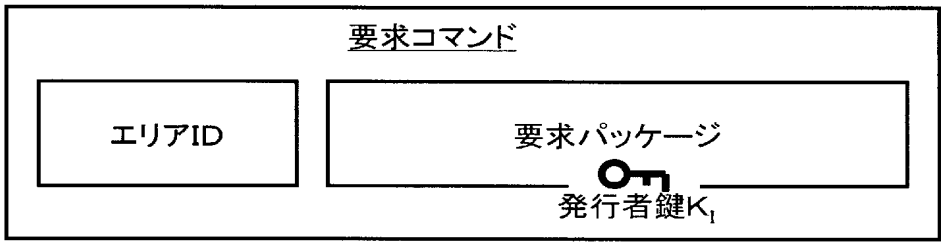

新規サービス提供元事業者
ICカード(OS)
ファイル・システムID要求(SC)
相互認証
デフォルトエリアID
鍵変更要求(エリアID, 鍵変更パッケージ)
鍵変更処理
ステータス
システム・コード変更要求
(エリアID, システム・コード変更パッケージ)
システム・コード
変更処理
ステータス
エリアID変更要求
(エリアID, エリアID変更パッケージ)
エリアID変更処理
ステータス

[図15]

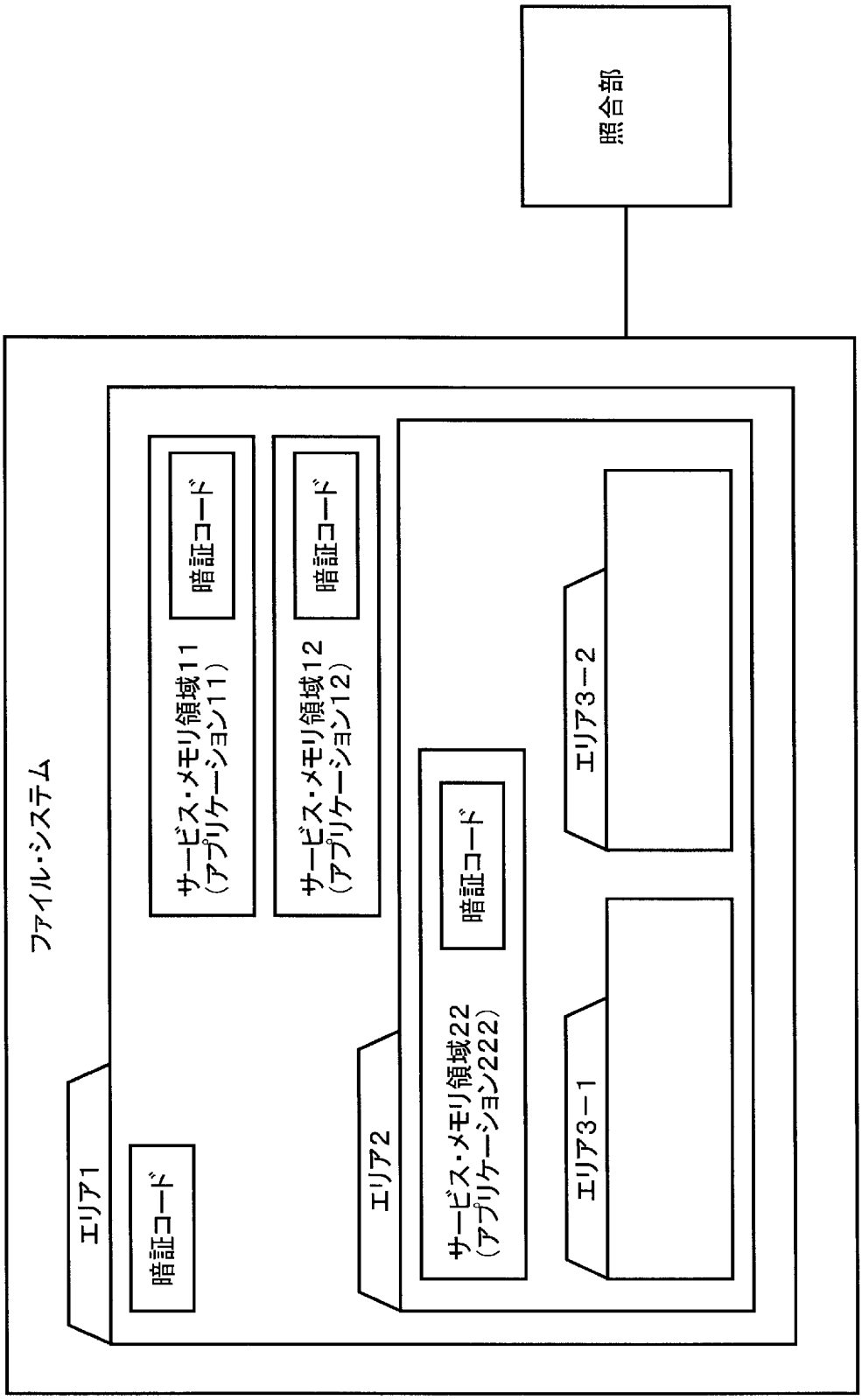
ファイル・システム＃0	＃1	＃1	＃1
システム・コードSD＃0	SD＃1	SD＃1	SD＃1
エリアID＃0	ID＃1	ID＃1	ID＃1
			

.....

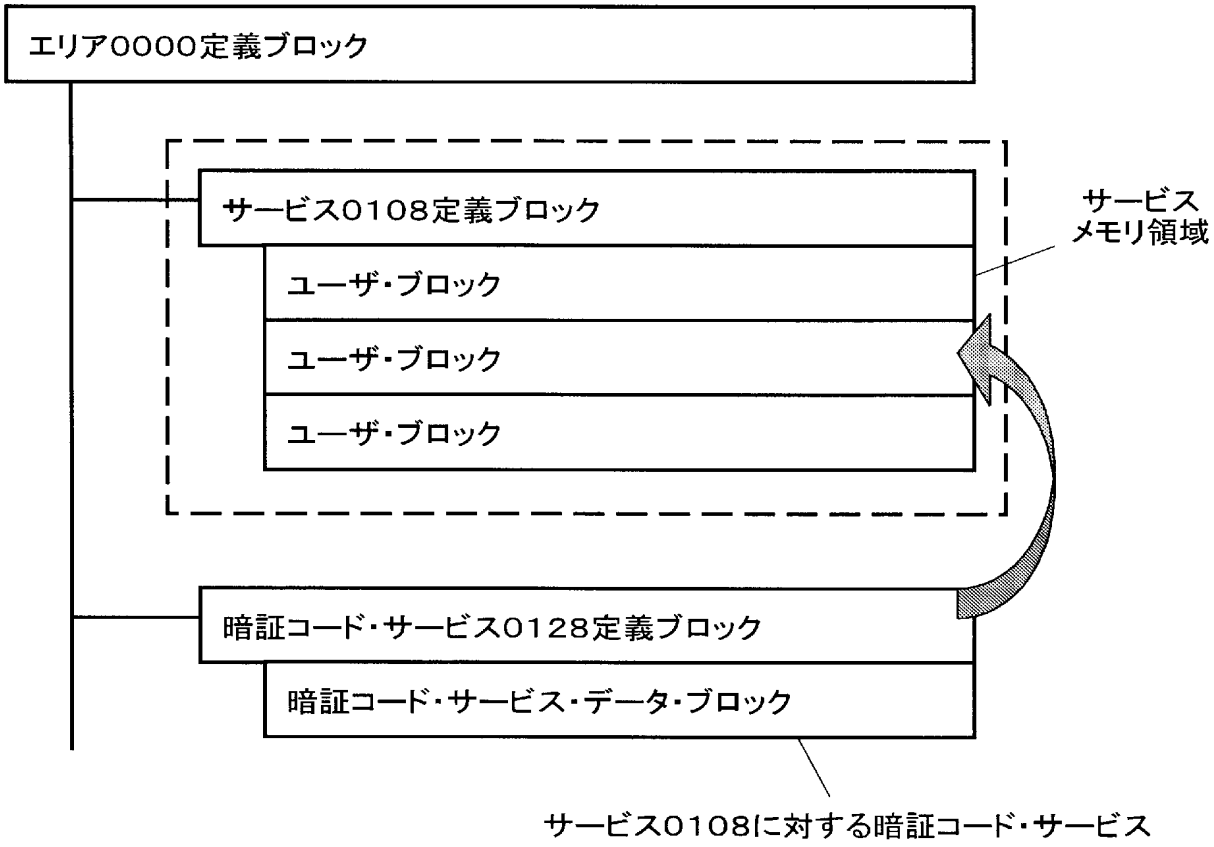
[図16]



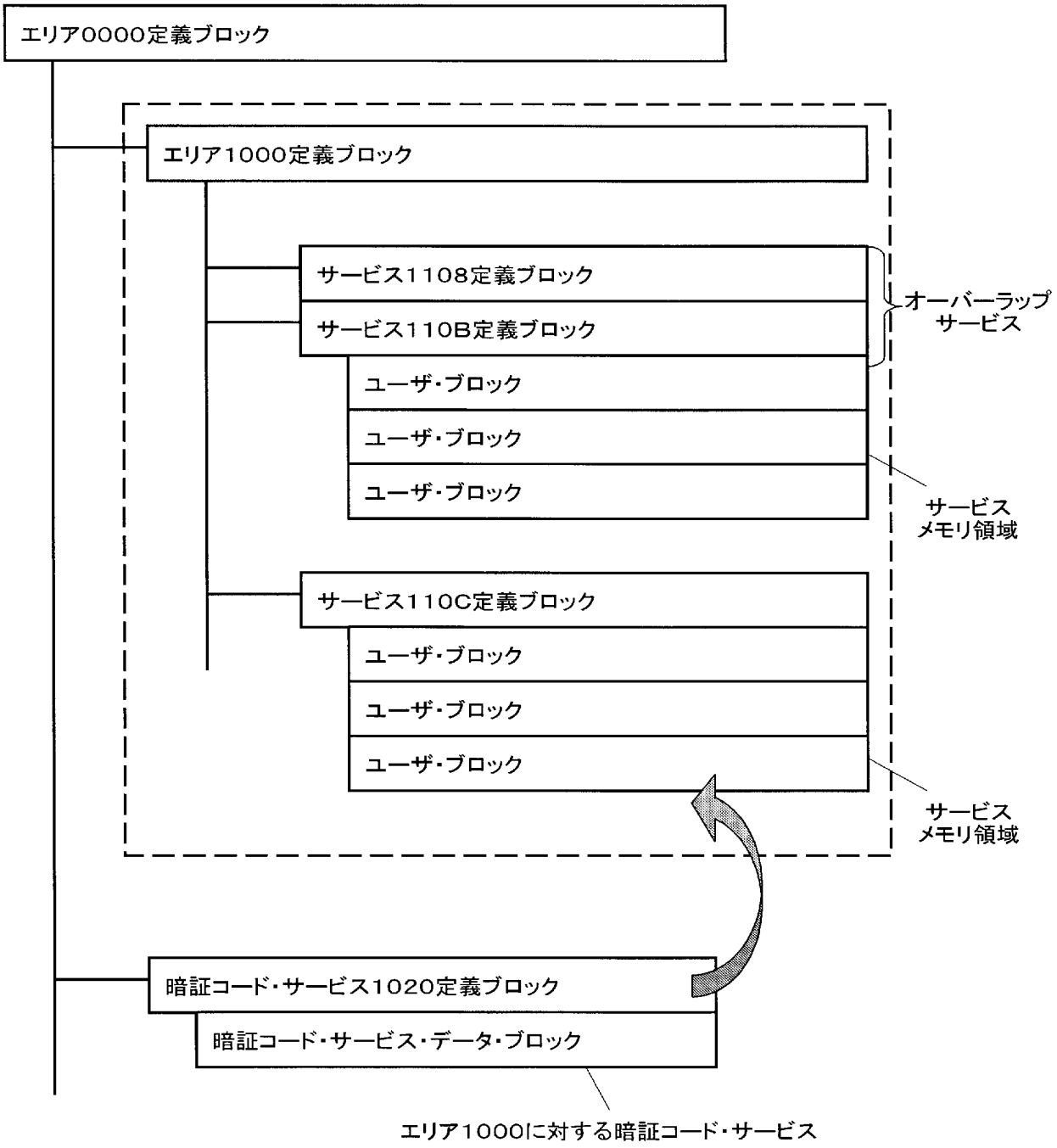
[図17]


照合部
ファイル・システム
エリア1
暗証コード
サービス・メモリ領域11
(アプリケーション11)
暗証コード
サービス・メモリ領域12
(アプリケーション12)
暗証コード
エリア2
サービス・メモリ領域22
(アプリケーション222)
暗証コード
エリア3－1
エリア3－2

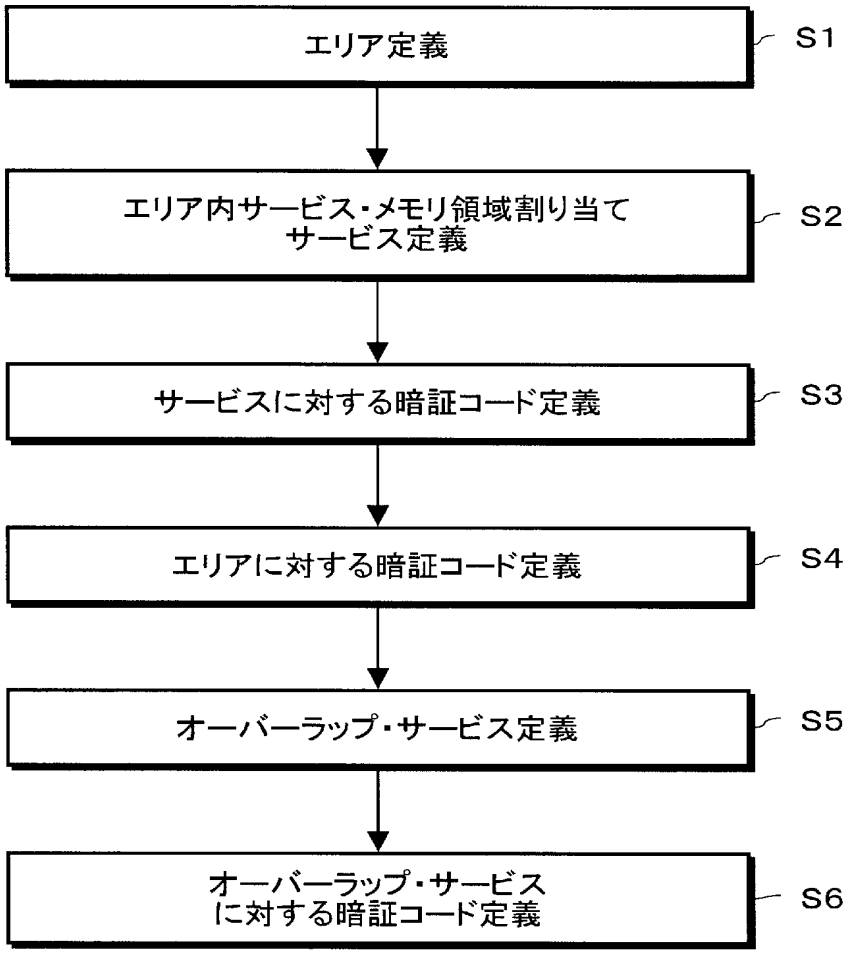
[図18]


エリア0000定義ブロック
サービス0108定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス0128定義ブロック
暗証コード・サービス・データ・ブロック
サービス0108に対する暗証コード・サービス

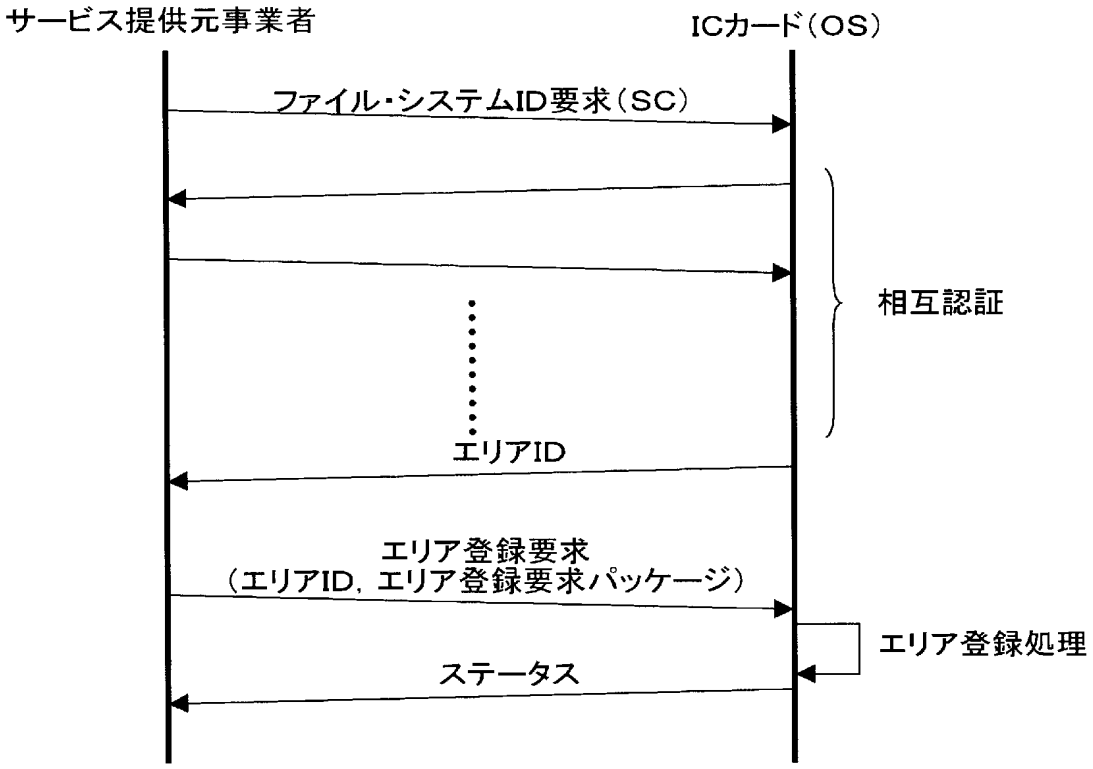
[図19]


エリア0000定義ブロック
エリア1000定義ブロック
サービス1108定義ブロック
サービス110B定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
オーバーラップ
サービス
サービス
メモリ領域
サービス110C定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス1020定義ブロック
暗証コード・サービス・データ・ブロック
エリア1000に対する暗証コード・サービス

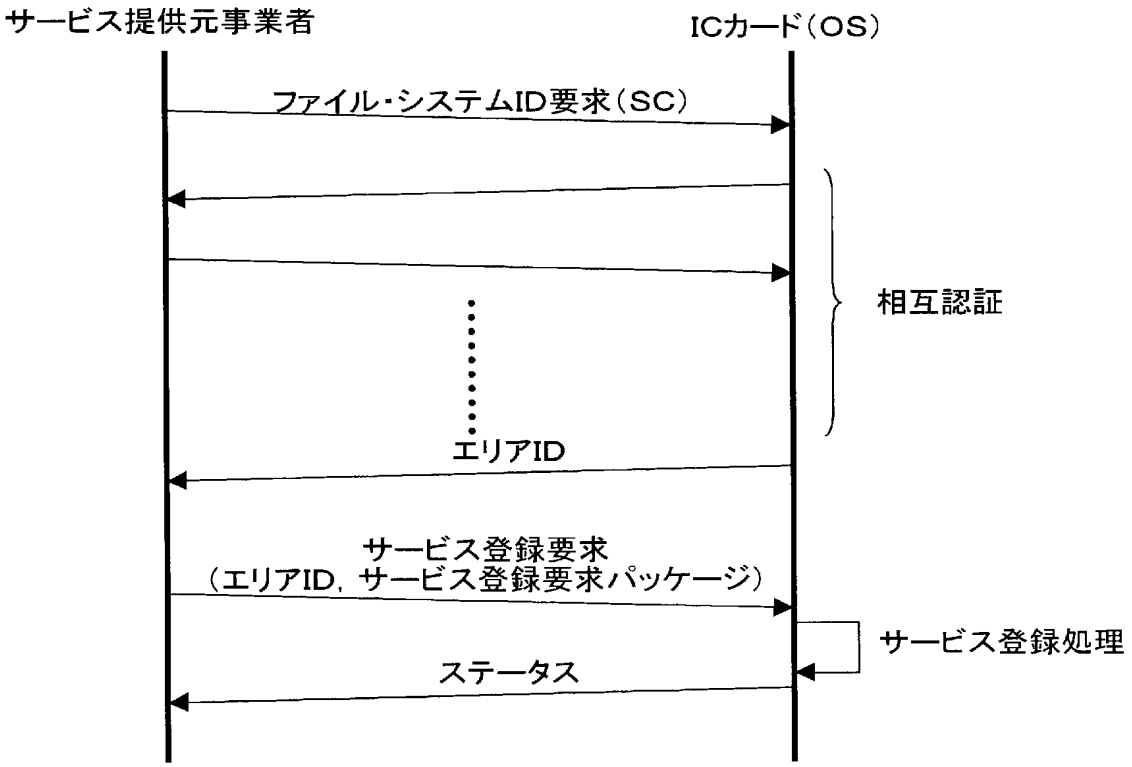
[図20]


エリア定義
S1
エリア内サービス・メモリ領域割り当て
サービス定義
S2
サービスに対する暗証コード定義
S3
エリアに対する暗証コード定義
S4
オーバーラップ・サービス定義
S5
オーバーラップ・サービス
に対する暗証コード定義
S6

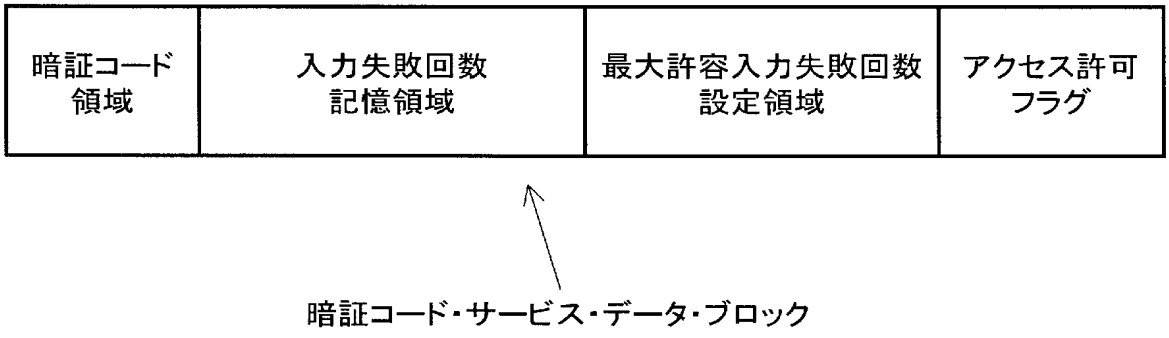
[図21]


サービス提供元事業者
ICカード（OS）
ファイル・システムID要求（SC）
相互認証
エリアID
エリア登録要求
（エリアID，エリア登録要求パッケージ）
エリア登録処理
ステータス

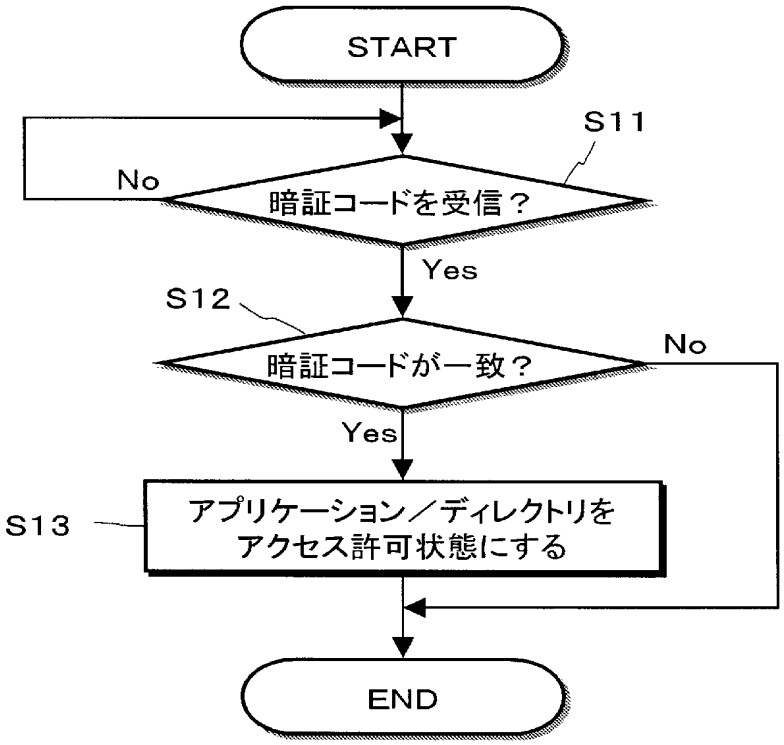
[図22]


サービス提供元事業者
ICカード（OS）
ファイル・システムID要求（SC）
相互認証
エリアID
サービス登録要求
（エリアID，サービス登録要求パッケージ）
サービス登録処理
ステータス

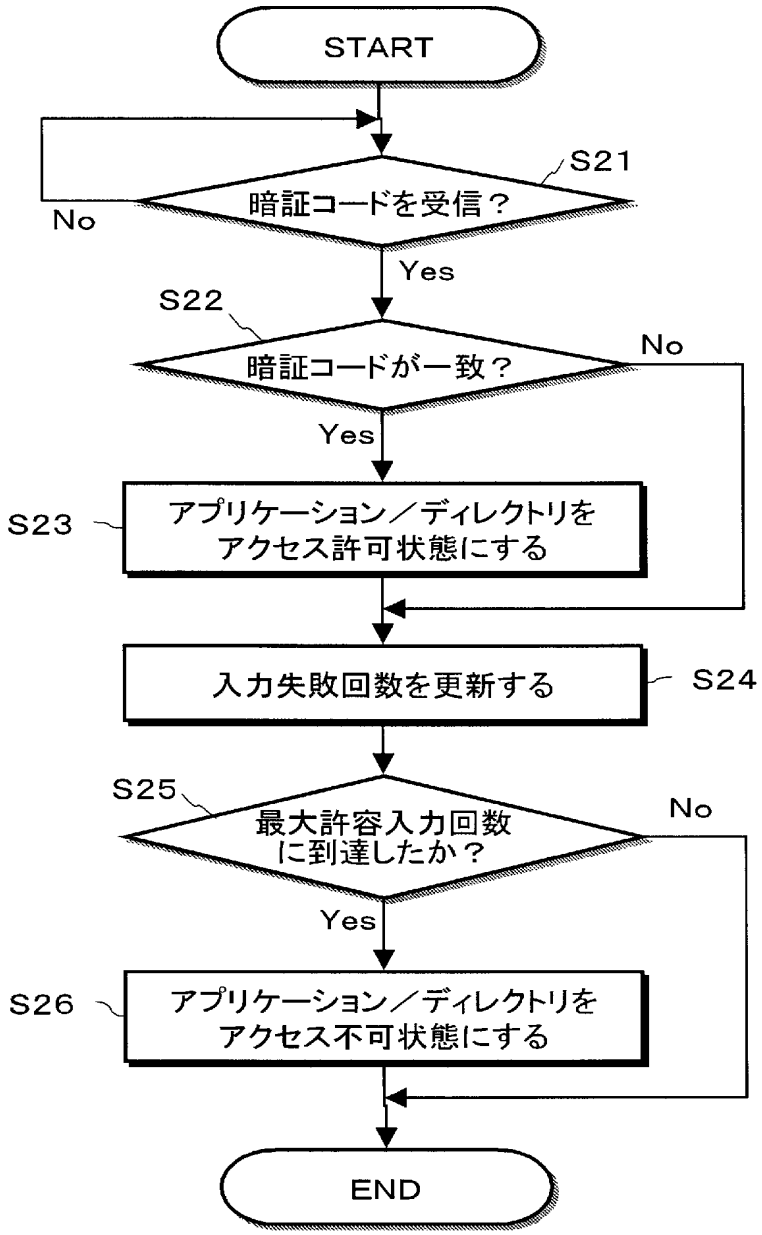
[図23]


暗証コード
領域
入力失敗回数
記憶領域
最大許容入力失敗回数
設定領域
アクセス許可
フラグ
暗証コード・サービス・データ・ブロック

[図24]


START
S11
No
暗証コードを受信？
Yes
S12
暗証コードが一致？
No
Yes
S13
アプリケーション／ディレクトリを
アクセス許可状態にする
END

[図25]


START
S21
暗証コードを受信？
No
Yes
S22
暗証コードが一致？
No
Yes
S23
アプリケーション／ディレクトリを
アクセス許可状態にする
入力失敗回数を更新する
S24
S25
最大許容入力回数
に到達したか？
No
Yes
S26
アプリケーション／ディレクトリを
アクセス不可状態にする
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/019202

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06K17/00, G06K19/073, H04L9/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06K17/00, G06K19/073, H04L9/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-278838 A (Sony Corp.), 27 September, 2002 (27.09.02), All page; all drawings & WO 2002/076012 A1 & US 2003/149854 A1 & EP 1276271 A1	1-12
A	JP 6-222979 A (Dainippon Printing Co., Ltd.), 12 August, 1994 (12.08.94), All pages; all drawings (Family: none)	1-12
A	JP 6-222980 A (Dainippon Printing Co., Ltd.), 12 August, 1994 (12.08.94), All pages; all drawings (Family: none)	1-12

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 March, 2005 (18.03.05)	12 April, 2005 (12.04.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/019202

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 8-171517 A (Dainippon Printing Co., Ltd.), 02 July, 1996 (02.07.96), All pages; all drawings (Family: none)	1-12
A	JP 2001-14441 A (Matsushita Electric Industrial Co., Ltd.), 19 January, 2001 (19.01.01), All pages: all drawings & WO 2000/065602 A1 & US 2003/221103 A1 & EP 1050887 A1	1-12
A	JP 10-105472 A (Toshiba Corp.), 24 April, 1998 (24.04.98), All pages; all drawings & US 5929428 A & EP 798674 A2	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１９２０２

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int. Cl.[7]　G06F12/14, G06K17/00, G06K19/073, H04L9/10

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int. Cl.[7]　G06F12/14, G06K17/00, G06K19/073, H04L9/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2002-278838 A（ソニー株式会社）2002.09.27, 全頁, 全図 & WO 2002/076012 A1 & US 2003/149854 A1 & EP 1276271 A1	1-12
A	JP 6-222979 A（大日本印刷株式会社）1994.08.12, 全頁, 全図（ファミリーなし）	1-12
A	JP 6-222980 A（大日本印刷株式会社）1994.08.12, 全頁, 全図（ファミリーなし）	1-12

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 18.03.2005	国際調査報告の発送日　12.4.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｎ　３０４４ 高橋　克 電話番号　０３－３５８１－１１０１　内線　３５８５

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 8-171517 A（大日本印刷株式会社）1996.07.02, 全頁，全図（ファミリーなし）	1-12
A	JP 2001-14441 A（松下電器産業株式会社）2001.01.19, 全頁，全図 & WO 2000/065602 A1 & US 2003/221103 A1 & EP 1050887 A1	1-12
A	JP 10-105472 A（株式会社東芝）1998.04.24, 全頁，全図 & US 5929428 A & EP 798674 A2	1-12